A Survey on Human-Centric Communications in Non-Cooperative Wireless Relay Networks

Behrouz Jedari, Feng Xia, *Senior Member, IEEE*, and Zhaolong Ning

***Abstract*—The performance of data delivery in wireless relay networks (WRNs), such as delay-tolerant networks and device-to-device communications heavily relies on the cooperation of mobile nodes (i.e., users and their carried devices). However, selfish nodes may refuse to relay data to others or share their resources with them due to various reasons, such as resource limitations or social preferences. Meanwhile, misbehaving nodes can launch different types of internal attacks (e.g., blackhole and trust-related attacks) to disrupt the normal operation of the network. Numerous mechanisms have been recently proposed to establish secure and efficient communications in WRNs in the presence of selfish and malicious nodes (referred as non-cooperative WRNs). In this paper, we present an in-depth survey on human-centric communication challenges and solutions in the non-cooperative WRNs that focuses on: 1) an overview of the non-cooperative WRNs and introduction to various types of node selfish and malicious behaviors; 2) the impact analysis of node selfish and malicious behaviors on the performance of data forwarding and distribution; 3) selfish and malicious node detection and defense systems; and 4) incentive mechanisms. Finally, we discuss several open problems and future research challenges.**

***Index Terms*—Opportunistic routing, D2D communications, social-awareness, resource allocation, user selfishness, malicious behaviors, attack detection, incentive mechanisms.**

I. Introduction

TODAY, individuals primarily use their handheld devices, such as smartphones and tablets for daily business communications and entertainment (*e.g.,* mobile advertising, file sharing, and gaming), which leads to exploding traffic over mobile networks. The global cellular traffic reached 7.2 exabytes per month at the end of 2016, and it is expected to grow to 49 exabytes per month by 2021 [1]. Thus, it has become a great challenge for the Internet providers and mobile network operators to serve the booming traffic demand of cellular networks. Meanwhile, mobile users in emergency scenarios may not have access to the Internet due to some reasons, such as limited coverage of cellular networks (*e.g.,* 3G or LTE). To overcome these problems, wireless relay networks (WRNs) have emerged as a promising communication paradigm in which the architecture of delay-tolerant networks (DTNs) [2], [3] is incorporated to establish device-to-device (D2D) communications [4] between mobile nodes (*i.e.,* users and their devices). In WRNs, nodes in proximity can opportunistically communicate and share their resources with each other using short-range and high-speed wireless interfaces, such as Wi-Fi and LTE Direct, which can significantly reduce the traffic of the cellular network. For instance, mobile social networks (MSNs) [5] have emerged as a novel networking paradigm in WRNs wherein the nodes' social relationships and contextual information are leveraged to enhance their communications and improve the resulting network performance. WRNs have many applications in different areas, such as mobile data offloading [6], proximity services [7], public safety communications [8], and vehicular networks [9], [10].

The primary goal of data forwarding and sharing protocols in WRNs is to exploit the nodes' contact, context, and social information to improve the data delivery performance in terms of different metrics (*e.g.,* delivery ratio, delay, overhead, and energy consumption). The majority of existing protocols assume that mobile nodes willingly participate in data delivery, share their resources with each other, and follow the rules of underlying networking protocols. Nevertheless, rational nodes in real-world scenarios have strategic interactions and may exhibit selfish behaviors due to various reasons (such as resource limitations, the lack of interest in data, or social preferences). For example, in case a node has limited battery resources or the cost of the network bandwidth delivered by mobile network operators is high, it would not be willingly to relay data for others until appropriate incentives are provided. Meanwhile, malicious nodes may attack the network in different ways to disturb the normal operation of the data transmission process. An adversary, for example, may drop received messages but produce forged routing metrics or false information with the aim of either attracting more messages or decreasing its detection probability. This issue becomes more challenging when some colluding attackers boost their metrics to deceive the attack detection systems. However, dealing with the non-cooperative behaviors of mobile nodes in WRNs is very challenging because of the distributed network model and intermittent node access to centralized authorities.

Recently, extensive analytical and simulation-based experiments have been conducted to study the effects of mobile nodes' selfish and malicious behaviors on the performance of data forwarding and dissemination in DTNs and D2D communications underlying cellular network. Besides, several distributed algorithms have been proposed to detect the nodes'

Manuscript received February 5, 2017; revised August 15, 2017 and November 26, 2017; accepted January 1, 2018. Date of publication January 9, 2018; date of current version May 22, 2018. This work was supported by the National Natural Science Foundation of China under Grant 61572106 and Grant 61502075. *(Corresponding author: Feng Xia.)*

The authors are with the Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, School of Software, Dalian University of Technology, Dalian 116620, China (e-mail: f.xia@ieee.org).

Digital Object Identifier 10.1109/COMST.2018.2791428

selfish and malicious behaviors and protect the network against malicious attacks. Furthermore, a large number of incentive mechanisms, such as reputation and rewarding approaches have been developed in both DTNs and D2D communications to either exclude selfish nodes from the data delivery process or stimulate them to participate in data relaying.

A. Prior Related Surveys

In the past few years, some survey articles have been presented in the context of WRNs. The majority of existing studies address the design requirements, platforms, and applications of DTNs and MSNs [5], [11]–[14]. For instance, Kayastha *et al.* [11] categorize MSNs into two types: infrastructure-based and infrastructure-less (or opportunistic) and discuss their architectures and characteristics. A number of studies review data routing and dissemination protocols in DTNs and MSNs [15]–[19] and categorize them into different classes according to various factors (*e.g.,* contact, context, and social features). Youssef *et al.* [20] explore different routing metrics, and Abdelkader *et al.* [21] evaluate the performance metrics of some well-known opportunistic routing protocols. Zhu *et al.* [22] study the positive (*e.g.,* social similarity and centrality) and negative (*e.g.,* user selfishness) aspects of data delivery algorithms in MSNs. Batabyal and Bhaumik [23] and Pirozmand *et al.* [24] study the impact of human mobility on the performance of opportunistic routing protocols. The authors in [25]–[27] respectively explore human behavior in social, temporal, and microblog networks. Silva *et al.* [28] study different cooperative strategies and their applications in challenged networks. The authors in [29]–[31] study design challenges of incentive strategies and their trade-offs for data forwarding in wireless networks. Furthermore, Ahmed *et al.* [32] study the services, technologies, and applications of event-based MSNs.

Recently, some articles study recent advances in D2D communications. Asadi *et al.* [4] classify D2D communications into in-band and out-band, *i.e.,* communication on the cellular and unlicensed spectrum, respectively, where the main difference is the interference caused by D2D nodes. Wang *et al.* [33] investigate the key components and architecture of D2D-based proximity services in MSNs and highlight their challenges and existing solutions. Zhao and Song [34] provide an overview of social-aware data dissemination approaches in MSNs and D2D communications with respect to game theory, matching theory, and optimization techniques. Gandotra *et al.* [35] study the implementation challenges of D2D communications from several aspects, such as resource allocation and interference management. In addition, Ahmed *et al.* [36] study resource allocation approaches in social-aware D2D communications with respect to their channel information, communication type, and networking technologies.

A couple of survey articles have explored security aspects of human-centric communications in WRNs. Najaflou *et al.* [37] study safety challenges in MSNs in three main groups: security, trust, and privacy. Liang *et al.* [38] provide a brief overview of MSN applications with respect to security and privacy and highlight some future research challenges about secure routing and denial-of-service attacks in MSNs. Furthermore, Zhang *et al.* [39] study various types of Sybil attacks and their defense mechanisms in a broad context of wireless networks. Haus *et al.* [40] present a survey on privacy and security in D2D communications. Despite the fact that the existing studies have outlined different aspects of WRNs, there is no prior in-depth survey of communication challenges and solutions in non-cooperative WRNs.

B. Contributions of This Survey

To the best of our knowledge, this paper is the first survey that provides a comprehensive review of existing work on human-centric communications in non-cooperative WRNs. Our major contributions can be summarized as follows:

- We present an overview of non-cooperative WRNs and introduce mobile nodes' different selfish behaviors and attack models.
- We survey recent studies that explore the impact of nodes' selfish and malicious behavior on the performance of data forwarding and distribution protocols in WRNs and explore their detection and defense mechanisms.
- We study numerous incentive mechanisms in WRNs and discuss their important characteristics.
- We discuss several open issues and highlight future research directions regarding data forwarding and distribution in non-cooperative WRNs.

C. Methodology

The main goal of this survey is to provide a structured and comprehensive overview of human-associated communications in non-cooperative WRNs. In particular, we explore data delivery in proximity-based networks under the circumstances that some mobile nodes exhibit selfish and malicious behavior to either maximize their utility or disrupt the data delivery process. In Section II, we present an introduction to non-cooperative WRNs with the aim of motivating the emergence of protocols and mechanisms to deal with non-cooperative behaviors in WRNs. Furthermore, we outline different forms of nodes' selfish and malicious behavior in data forwarding. Next, we study data delivery challenges and solutions in non-cooperative WRNs from three perspectives. In Section III, we study proposals that analyze the impact of nodes' selfish behaviors on the performance of data delivery protocols. In particular, we categorize existing methods into simulation-based, theoretical, and hybrid methods and highlight their principal solutions, specialties, and limitations in Table I.

In Section IV, we study selfish and malicious node detection and isolation algorithms in WRNs where they aim to secure data delivery protocols against nodes' non-cooperative behaviors. We categorize the selfish node detection and isolation methods into two classes (watchdog systems and social trust-based systems) and highlight their major contributions, properties, and limitations in Table II. Next, we explore proposals that aim to detect different types of node attacks in WRNs and outline their principal contributions, major properties, and shortcomings in Table III. In Section V, we study

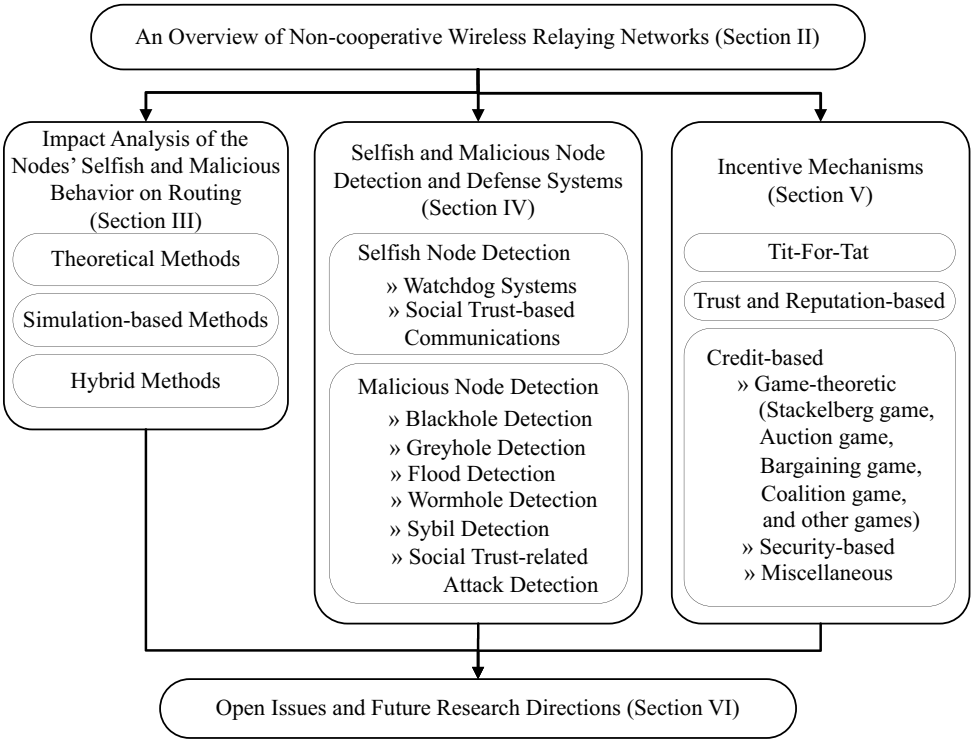

Fig. 1. The organization of the remaining parts of the paper.

incentive mechanisms that aim to promote the cooperation of nodes in data relaying where we categorize existing methods into three main classes: Tit-For-Tat, reputation-based, and credit-based mechanisms. First, we introduce prominent Tit-For-Tat and credit-based schemes and outline their major characteristics in Table IV. Next, we classify credit-based mechanisms into three classes (game-theoretic, security-based, and miscellaneous) and highlight their principal solutions, incentive objects, and limitations in Tables V and VI. We believe that this paper can educate the research community and networking protocol designers how to effectively deal with non-cooperative behaviors of mobile carriers in next-generation wireless networks.

The rest of the paper is organized as follows (Fig. 1). Section II provides an overview of non-cooperative WRNs and introduces various selfishness and attack models. Section III introduces different approaches that study the impacts of node selfish and malicious behavior on the performance of data forwarding and sharing protocols in WRNs. Section IV discusses the selfish node detection techniques and attack defense systems. Section V studies representative incentive mechanisms that aim to either promote the cooperation of selfish nodes or exclude them from the data delivery process. Section VI provides several open problems and future research directions, and Section VII draws the conclusion.

II. An Overview of Human-Centric Communications in Non-Cooperative WRNs

Fig. 2 illustrates an overview of human-centric communications in non-cooperative WRNs. As shown in the figure, mobile nodes (or user equipments) in proximity can establish peer-to-peer communications to exchange data with each other using short-range and high-speed wireless transmission technologies (such as Bluetooth, ZigBee, WiFi-Direct or LTE Direct) [41]. The communication between the nodes can be in standalone D2D mode (or ad hoc mode) autonomously or via network-assisted D2D communications with the control of base stations (BSs) or core network. Meanwhile, the nodes may sporadically have access to the Internet and service providers (such as a trusted third party or credit clearance center) via BSs or Wi-Fi hotspots. In this setting, the nodes' social ties and relationships captured from their online social network profiles or the nature of their mobility (*e.g.,* contact patterns or geographic information) can be leveraged to enhance their communications and capacity of the network.

Cooperative communications can improve the performance of data delivery in WRNs and offload the traffic of the cellular network. For example, mobile devices in D2D communications can cache popular content received from the cellular network and share them with interested neighbor requestors, which can improve the data delivery performance, increase the network capacity, and offload the traffic of BSs. However, some nodes might exhibit selfish behavior and refuse to relay messages received from all or some other nodes or share their resource with them because of different reasons, such as limited resources (*i.e.,* buffer, bandwidth, and energy resources) or monetary cost. In addition, malicious nodes can launch different forms of attacks, such as manipulating and diffusing wrong information to deceive the nodes and disturb their normal communications. Thus, we can classify mobile nodes into three types: cooperative, selfish, and malicious nodes. In general,

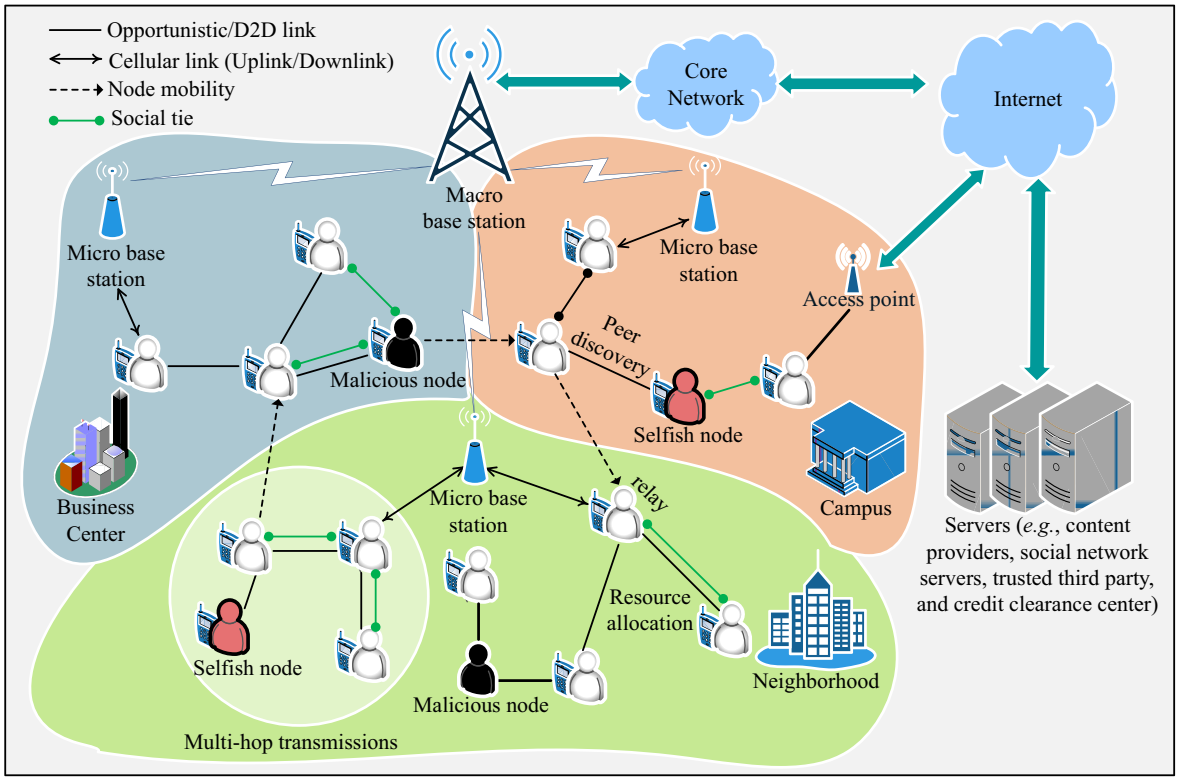

Fig. 2. An overview of non-cooperative wireless relay networks.

the cooperative nodes follow the rules of the underlying networking protocols, whereas the selfish nodes consume the network resources but refuse to provide services for all or some other nodes with the aim of maximizing their own benefits. Besides, the malicious nodes attack the network in different ways to disrupt the network normal functionalities. In the rest of this section, we explain social-awareness communications in WRNs and compare the characteristics of DTNs and D2D communications. Next, we discuss different selfish behaviors and malicious attacks that can be launched by non-cooperative nodes in WRNs.

A. Social-Aware Communications in WRNs

Mobile nodes' implicit (*e.g.,* mobility information) and explicit (*e.g.,* online social network information) social characteristics and relationships can accurately mirror their interactions and relationships in the real life. Hence, socially-aware wireless networking has emerged as a promising solution to optimize various aspects of human-centric communications in WRNs [42]–[46]. In particular, nodes' different social characteristics, such as social ties, community, and centrality are primarily exploited to enhance different key technological problems in cooperative communications underlying cellular network [47], [48]. For instance, nodes' social network and mobility information can be leveraged to select appropriate relay nodes in D2D communications with the aim of improving the data delivery success ratio while minimizing the communication overhead (see [49], [50]). In addition, nodes' social characteristics are exploited to address peer discovery [51] and resource allocation [52] in D2D communications.

In contrast to cooperative networks, the social information of mobile nodes can also be exploited to achieve secure communications in non-cooperative WRNs. For instance, social-based trust or reciprocity relationships between interacting parties can streamline data delivery performance and protect their communication against malicious attacks (see [53], [54]). In addition, the social features and behaviors of nodes can help detect their possible selfish and malicious actions [55]. Furthermore, utilizing nodes' social features can help model their interactions and incentive mechanisms realistically with respect to their similar and conflicting interests [56]. In this paper, we particularly study proposals that leverage nodes' social attributes and relationships across different aspects of their communications in non-cooperative WRNs.

B. DTNs and D2D Communications

Although mobile carriers in both DTNs and D2D communications can establish opportunistic contacts to exchange their messages, there are some distinct differences in the form of their communications. Typically, there is no permanent cellular infrastructure in DTNs and the research question is how to efficiently deliver a message from a source node to its destination node by choosing appropriate relay nodes. In contrast, the main goal in D2D communications is to efficiently offload the traffic distributed by a cellular network through D2D devices to interested nodes, which is applicable in new business models and scenarios (*e.g.,* pervasive social networks and location-based services). In other words, there is no strict publish/subscribe model in DTNs in comparison with the data offloading mechanisms assumed in D2D communications. In

addition, DTNs primarily employ multi-hop relaying to deliver messages to destination nodes, whereas D2D communications apply single-hop or multi-hop cluster-based transmissions. Furthermore, mobile nodes in DTNs communicate with each other on an unlicensed spectrum, which is performed by the devices autonomously. In contrast, D2D devices can use both licensed and unlicensed spectrum under the controlled of the BS or within the cooperation between the BS and encountered nodes, which can cause D2D-to-cellular and cellular-to-D2D interference [57]. Hence, resource allocation, peer discovery, mode selection, and power management are major challenges in D2D communications [58].

C. Node Selfishness Models

Although cooperation among mobile nodes in proximity can improve the data delivery performance in WRNs, some nodes may exhibit selfish behavior and do not share their resources with other nodes altruistically with the aim of maximizing their preferred utility. The selfish behavior of mobile carriers could have different reasons, such as resource constraints, the lack of interests in messages, privacy concerns, or social preferences. For example, in case a mobile node has limited battery resources or the cost of network bandwidth delivered by mobile network operators is high, it may not be willing to consume its resources and relay data for all or some other nodes until appropriate incentives are provided.

Different forms of node selfishness models have been considered in the literature. Hui *et al.* [59] propose different altruism distributions, such as uniform, degree-biased, and community-biased to realize human selfish behaviors in WRNs. Some studies identify a *probabilistic selfish behavior* in which a selfish node may not participate in relaying a message according to a probabilistic function. A number of studies (*e.g.,* [60]) define *non-forwarding* and *partially-forwarding* selfish actions where a selfish node does not relay messages to other nodes or only delivers the relaying messages to their destination nodes. Panagakis *et al.* [61] introduce *non-copying* (or dropping) and *non-forwarding* selfish behavior. In addition, Kouyoumdjieva and Karlsson [62] define two types of selfish nodes: strict and mild. A strict selfish node turns off its radio interface after receiving its requested data items, whereas a mild selfish node cooperates with others for a limited time even after receiving its requested data. Besides, Ip *et al.* [63] introduce egotistic nodes, which change the range of their communication signals in different situations.

Despite various selfishness models and actions mentioned above, a vast number of existing studies in non-cooperative WRNs have explored the role of nodes' social relationships and preferences in their selfish behavior. Following the homophily phenomenon in sociology, it is revealed that mobile nodes usually provide better services for those with whom they have strong social relationships or similarities. For example, nodes with similar interests and backgrounds tend to cooperate with each other in data delivery, even if they have not had direct contact with each other previously [64], [65]. Thus, two types of selfish nodes can be defined as follows.

- *Individually Selfish (IS) nodes:* IS nodes have socially-oblivious selfish behavior and exhibit a uniform selfish behavior to other nodes without considering the utility of the nodes with whom they have social relationships or common interests. For example, an IS node does not consider the benefits of its friends in data sharing and provides better services for nodes with early access times.
- *Socially Selfish (SS) nodes:* SS nodes alleviate the degree of their selfishness degree based on their social relationships or similarities to provide better services to their friends or nodes with whom they have strong social ties. In contrast, they are unwilling to provide forwarding services for strangers or nodes with different social objectives or preferences with the aim of saving their buffer and energy resources. For example, SS nodes in community-based DTN or D2D data offloading scenarios are willing to cache and deliver messages to nodes in the same community but refuse to relay the messages to nodes in other communities.

D. Social Trust

Social trust is a powerful descriptor of friendship, honesty, security, and integrity that can secure interactions between mobile nodes in wireless networks. In particular, due to the lack of a permanent central authority in WRNs, establishing social trust relations between nodes (by leveraging their online social network information, direct, and indirect interactions) can promote trustworthy cooperation among them and protect them against threats and attacks [66]. For example, social trust can improve the performance of D2D communications by asking the most trustworthy nodes in proximity (*e.g.,* family members, friends, or colleagues) to relay messages [67]. In contrast, the lack of trust can make the nodes reluctant to cooperate with each other due to different reasons ranging from privacy concerns (*e.g.,* not trusting to interact with strangers) to resource constraints (*e.g.,* energy and buffer limitations). However, malicious nodes can attack the trust system, for example, by exaggerating the reputation of other malicious nodes or submitting bad recommendations against trustworthy nodes [68], [69]. We study several recently proposed social trust-based communications in Section IV.

E. Node Attack Models

Opportunistic communications and interactions among mobile nodes in proximity are vulnerable to different types of attacks (*e.g.,* physical attacks, compromised credentials, and protocol attacks) due to the open architecture of the network, node mobility, and privacy issues. To deal with network attacks, numerous protection and defense mechanisms have been designed to guaranty the requirements of a secure communication, such as authentication, availability, confidentiality, and integrity. Despite various attack and defense mechanisms discussed in the literature, in this paper, we focus on different forms of internal attacks (*i.e.,* the attacks launched by nodes with valid cryptographic credentials) that can disrupt the normal communications between the nodes and the network throughput severely.

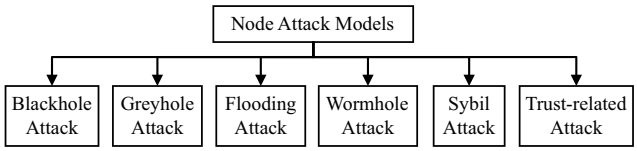

Fig. 3. Different types of node attacks in wireless relay networks.

As shown in Fig. 3, we categorize attacks launched by malicious mobile nodes into the following types:

- *Blackhole Attack:* a blackhole adversary drops received messages even if it has free buffer space to store them but produces forged metrics (*e.g.,* message delivery probability) to attract more messages or hide its real identity.
- *Greyhole Attack:* a particular type of blackhole attack in which a greyhole adversary drops a fraction of received messages even if it has free buffer space but produces forged metrics that makes it difficult for other nodes to detect it. In a complex form of the greyhole attack, the attacker drops some received messages and injects other fake messages instead.
- *Data Flooding Attack:* a data flooding attacker injects as many messages as possible into the network to overuse the network resources (*e.g.,* bandwidth, energy, and buffer) and degrade the throughput. A flooding attacker can attack the network in different ways. For example, it may generate fake messages or copy the same message destined for random or selective target nodes through some victim relay nodes that have the highest popularity. In certain cases, a flooding attacker may destine its fake messages to non-existing nodes in order to make them remain in the network longer.
- *Wormhole Attack:* a wormhole adversary receives messages in one location of the network and then moves and replicates them to nodes in another part of the network in order to pretend that messages are transferred through fewer transmission hops. The main objective of a wormhole attacker is to disarrange the topology views of the network by providing fake neighboring information and improve its position (*e.g.,* its reputation).
- *Sybil Attack:* a Sybil attacker (or Sybil) generates a large number of bogus identities or location information to establish many fake links in the network with the aim of manipulating its reputation or the bad reputation of other nodes [39]. For example, a Sybil attempts to disseminate spam and advertisements, produce wrong reports, obtain a disproportionately high benefit from the network without sufficient contribution, and steal the other nodes' private information. In some cases, a mobile Sybil may contact other nodes to share the same social or location information with different forged identities and mislead their routing decisions. Dealing with the Sybil attack becomes more challenging when compromised colluding nodes augment the capability of Sybils.
- *Social Trust-related Attacks:* a malicious node can attack a trust management mechanism in different ways to disrupt its functionality. For example, it can launch a self-promoting attack to improve its importance and be selected as the service provider or relay node, but then it refuses to provide the service or provide a malfunctioned service. In addition, malicious nodes can launch other types of trust-related attacks (such as bad-mouthing or ballot stuffing attacks [69]) in the form of recommendations to exaggerate the trust level of their friends or ruin the reputation of unknown strangers or well-behaved nodes. Thus, a robust trust management mechanism should be designed to protect the trust level of nodes against such attacks.

F. Common Data Delivery Protocols to Evaluate Human Non-Cooperative Behaviors in WRNs

In general, data forwarding and dissemination protocols in WRNs employ multi-copy replication mechanisms to improve the data delivery probability with the cost of communication overhead. Broadly, multi-copy replication mechanisms can be classified into two major classes: *stateless* and *deterministic*. In the stateless protocols (*e.g.,* Epidemic [70], Two-hop [71], spray and wait (SnW) [72], and backpressure-based routing [73]), mobile nodes make data replication decisions locally without considering the properties of other nodes (*e.g.,* their delivery probability). In contrast, in deterministic protocols, the nodes' contact history (*e.g.,* Prophet [74]) or social features (*e.g.,* Bubble Rap [75], dLife [76], and PIS [77]) are utilized to choose optimal intermediate nodes and improve the data forwarding performance in terms of important metrics, such as data delivery ratio, delay, and communication overhead.

The majority of works we will discuss through the rest of this paper employ the stateless protocols to evaluate the performance and effectiveness of their solutions in non-cooperative WRNs. We believe that it is because implementing the stateless routing protocols is relatively straightforward. Additionally, the impact of nodes' different behaviors on data delivery performance can be well demonstrated using the stateless protocols.

III. Impact of Node Selfish Behavior on Opportunistic Communications

Different forms of nodes' selfish behavior can influence the data delivery performance metrics (*e.g.,* data delivery ratio, delay, transmission cost, and resource consumptions) in different ways. For example, the message dropping or non-forwarding actions of selfish nodes in multi-copy routing protocols can increase the delivery delay but improve the delivery overhead. Moreover, selfish nodes can highly degrade the efficiency of data offloading in D2D communications, especially when seed nodes refuse to deliver the content to non-seed nodes via opportunistic communications. In the literature, different models and techniques have been employed to characterize and estimate how routing metrics change in the presence of non-cooperative nodes. We categorize the impact analysis methods into three classes: theoretical, simulation-based, and hybrid methods. In the following, we discuss the main contributions of each work and highlight their major results.

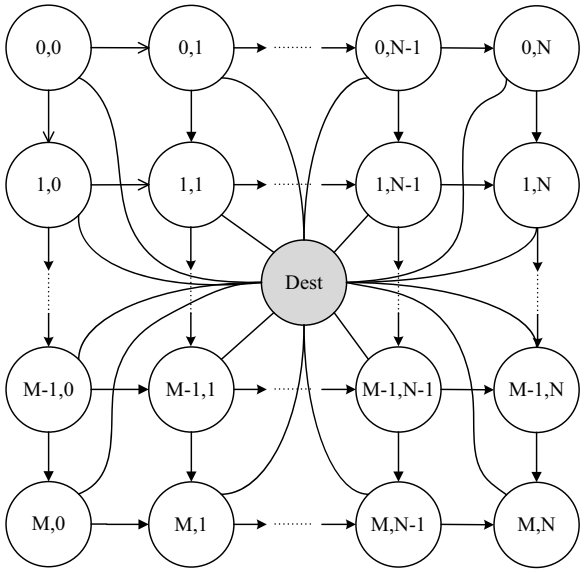

Fig. 4. A sample two-dimensional CTMC model for the Epidemic routing process with $(M+1) \times (N+1)$ transient states where state (0,0) is the initial state and state (Dest) is the absorbing state [78].

A. Theoretical Methods

Several analytical methods have been proposed to analyze the impact of nodes' selfish behavior on the performance of opportunistic communications. A considerable number of theoretical methods in this class have employed the continuous-time Markov chain (CTMC) model to analyze the data delivery process. In general, a CTMC model is characterized by a state space and a transition matrix where the process starts with an initial state and changes to another state according to the probabilities of particular transitions in the transition matrix. Fig. 4 shows a CTMC transition machine that models a message relaying in a network with two non-overlapping communities V_1, V_2 with N and M SS nodes, respectively. The transition process starts from state (0,0) which implies that the number of the message copies in communities V_1 and V_2 equals to 0. Once the number of the message copies is more than 0, the message may be transmitted to the destination state (Dest). Thus, a major question is how to obtain the transition probability from each state to state (Dest) that can help derive the message delivery performance metrics, such as the delivery delay and cost.

Karaliopoulos [79] formulate message relaying in the Epidemic and Two-hop protocols using a two-dimensional CTMC (2D-CTMC) model. In particular, *deceleration factor* metric is devised to measure the deterioration of the delivery delay, which is defined as the ratio of the expected delivery delay when there are K selfish nodes versus the case all the nodes are cooperative. The numerical results demonstrate that the delivery delay in both the protocols increases as the number of the selfish nodes goes up. Meanwhile, it is shown that both the protocols are resistant against the selfish behavior when it is probabilistic. For example, the deceleration factor remains below 2 even in the presence of 70% of selfish nodes with selfishness degree 0.5. Li *et al.* [80] design a 2D-CTMC model to obtain the message delivery delay and cost. The analytical results show that the non-forwarding and non-copying actions have opposite impacts on the Epidemic and Two-hop protocols. For instance, the non-copying action of selfish nodes increases the delivery delay and cost in Two-hop, whereas the delivery delay in Epidemic increases but the cost does not change considerably.

Resta and Santi [81] model the routing process in the Epidemic, Two-hop, and SnW protocols as a stochastic coloring process to derive the data delivery delay and communication cost metrics. In particular, three levels of node cooperation: fully cooperative, probabilistic cooperative, and non-cooperative behaviors are considered. Based on the coloring process, a node can be in three states: uncolored (has not received a message), colored active (has at least two copies of the message), and colored inactive (has only one copy of the message that can deliver to its destination). The coloring process finishes when the destination node receives the message and becomes colored. The results show that the data delivery performance doubles even when a small portion of nodes cooperates in message relaying in comparison to the case all the potential forwarders drop messages.

While the above-mentioned studies only consider the nodes' social-oblivious selfishness behavior, Li *et al.* [78] analyze the impact of SS nodes on the Epidemic routing where the network nodes are partitioned into two non-overlapping communities. In particular, a 2D-CTMC is employed to model the message relaying process. Besides, *delay deceleration ratio* and *cost enhancement ratio* metrics are introduced to measure the performance degradation of the data delivery delay and cost, respectively. The results demonstrate that as the number of selfish nodes increases, the delivery delay increases, but there is more reduction in the delivery cost. Xiao *et al.* [82] apply a 2D-CTMC model to explore how IS and SS nodes affect the performance of gossip-based data forwarding in DTNs. The network is partitioned into two non-overlapping communities where the nodes in only one community are IS. The results show that the non-forwarding action of IS nodes reduces the transmission cost more than increasing the delivery delay, whereas the non-copying action of IS nodes degrades the cost less than the delivery delay. Furthermore, the gossip-based forwarding is robust to social selfishness because the transmission cost decreases significantly at the cost of a slight increase in the delivery delay.

B. Simulation-Based Methods

Several existing studies employ simulations to explore the impact of node selfishness on data delivery performance. Keranen *et al.* [60] explore the impact of the nodes' non-forwarding and partially-forwarding actions on the performance of Epidemic, SnW, and Prophet protocols in terms of the data delivery ratio and delay. The experimental results demonstrate that DTNs tolerate a high percentage of non-cooperative nodes (20-40% or even 60%) without too much harm, even though they still utilize the other nodes' resources to deliver their own messages. Meanwhile, synthetic random mobility models are most vulnerable to less cooperation

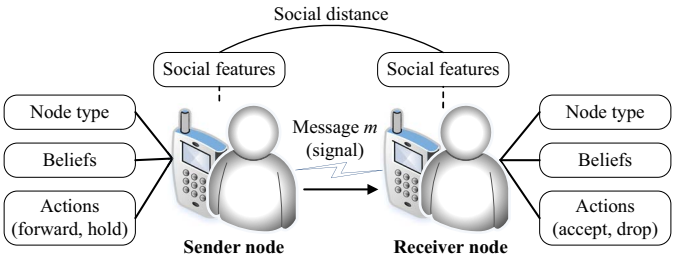

Fig. 5. The belief-based uncertain interaction between nodes in Sig4UDD.

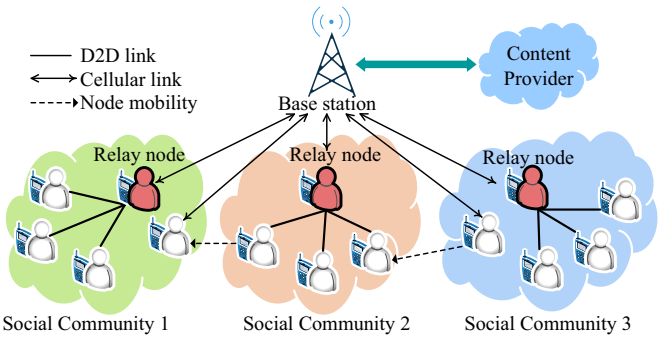

Fig. 6. Community-based D2D communications underlying cellular network in the presence of socially selfish relay nodes.

that implies that DTNs are robust against the nodes' non-cooperative behavior. Comparatively, it is revealed that the performance degradation of SnW is relatively higher than Epidemic and Prophet because SnW generates a limited number of message copies.

Hui *et al.* [59] study the impact of nodes' different altruistic distributions (such as the percentage of uniform, normal, degree-biased, and community-biased) on the performance of opportunistic communications. The experimental results reveal that a network setting with uniform, normal, or degree-biased distributions can achieve almost 90% performance of a fully cooperative network due to their multiple forwarding paths. In addition, it is confirmed that the community-biased traffic can further increase the robustness of the network. Kouyoumdjieva and Karlsson [62] evaluate the performance of a publish-subscribe data offloading system in the presence of the strict and mild nodes. The performance results in terms of the energy consumption and data delivery ratio demonstrate that in the presence of strict nodes, the energy consumption decreases significantly at the cost of losing some data delivery ratio. In contrast, under mild selfishness, the energy consumption further decreases while the delivery ratio increases.

While the studies above focus on the nodes' social-oblivious selfishness behavior, Bermejo *et al.* [83] study human altruism in AppExp and WebExp applications with respectively 800 and 737 nodes considering the nodes' remaining battery level and social tie information. The experiments show that nodes respectively exhibit 70% and 52% altruistic behavior in AppExp and WebExp when a minor credit (1 dollar) is awarded. Meanwhile, the nodes are not willing to relay data received from others when their remaining battery level is less than 10%. Xia *et al.* [84] explore the impact of IS and SS nodes on social-based routing protocols under uncertain node cooperation. In particular, a signaling game approach (Sig4UDD) is proposed where Bayesian Nash equilibrium and perfect Bayesian equilibrium are employed to analyze the nodes' one-stage and multi-stage interactions (Fig. 5). Meanwhile, a belief system is established to help the nodes predict the type of their encounters and decide whether to forward a message to them or not. The experimental results demonstrate that nodes in Sig4UDD can effectively establish their beliefs based on their previous interactions that can decrease the transmission cost significantly while improving the data delivery delay. Similar to [84], Wang *et al.* [85] employ random utility theory to model gossip diffusion of rational nodes in social networks under uncertainty. Next, a formal framework based on mean field theory is devised to analyze the diffusion process. The results demonstrate that small uncertainty can speed up gossip diffusing significantly.

A limited number of proposals study the impact of human selfish behavior on the performance of D2D communications. Wang *et al.* [86] consider an opportunistic data offloading approach in network-assisted D2D communications in which nodes download the contents from the BS and then decide whether to share them with other nodes or not according to their historical records. Next, a network formation game is designed to model the dynamic characteristics of the nodes' selfish behaviors wherein the gain and cost functions are specified for downloading content via D2D communications or cellular network. The simulation results show that the selfish behavior of nodes can degrade the offloading efficiency significantly. In addition, the cost ratio between the cellular and D2D transmissions, as well as the nodes' access delays and mobility patterns affect the performance gap significantly.

Wang *et al.* [87] study human selfish behavior in community-based D2D communications in which SS nodes in each community participate in relaying contents received from the BS to non-relay nodes with respect to their social relations, as shown in Fig. 6. The study adopts a bipartite graph to obtain a matching solution between the relay and non-relay nodes when the cooperation degree of relay nodes and the number of communities vary. The experiments show that SS nodes degrade the system throughput with fewer mobile devices. Besides, it is revealed that the highest performance gap occurs when the number of relay and non-relay nodes are equal. Similarly, Gao *et al.* [88] employ a time-varying graph model to study the impact of IS and SS nodes on the performance of data offloading in community-based D2D communications. It is assumed that a BS transmits data to a helper seed node and requests it to disseminate the data to the subscribers or other seed nodes. Nevertheless, a selfish seed node can exhibit selfish behavior in receiving contents from the BS or forwarding them to subscribers. The experimental results demonstrate that a few numbers of IS and SS nodes inside each community do not affect the network throughput considerably, especially in a network with a large number of communities.

C. Hybrid Methods

The majority of studies in this class employ theoretical approaches to model and analyze opportunistic data delivery

TABLE I
SUMMARY OF THE WORKS THAT STUDY THE IMPACT OF HUMAN SELFISH BEHAVIOR IN WIRELESS RELAY NETWORKS

Approach	Reference	Principle of proposed solutions	Selfish behavior		Evaluation parameters				Routing protocol			Specialties (+) and limitations (-)
			Individual	Social	Delay	Delivery	Cost	Energy	Epidemic	Two-hop	Others	
Theoretical	Karaliopoulos [79]	A 2D-CTMC to model the message relaying process	√	×	√	×	×	×	√	√	×	+ Considering both non-forwarding and non-copying selfish actions - Data delivery delay analysis only
	Li *et al.* [80]	A 2D-CTMC to model the message relaying process	√	×	√	×	√	×	√	√	×	+ the data delivery delay and cost tradeoff analysis - No comparison with previous works
	Resta and Santi [81]	A stochastic coloring process to model the message delivery	√	×	√	×	√	×	√	√	√	+ Extensive analysis of the effects of selfishness on delivery delay and cost - No comparison with previous work
	Li *et al.* [78]	A 2D-CTMC to model the message relaying process with social selfishness	×	√	√	×	√	×	√	×	×	+ Analyzing the impact of selfishness in community-based DTNs - Only evaluates the Epidemic routing
	Xiao *et al.* [82]	A 2D-CTMC model to analyze the gossip dissemination	√	√	√	×	√	×	√	×	×	+ Studying individual and social selfishness, and system energy - No comparison with previous work
Simulation-based	Keranen *et al.* [60]	Evaluating the non-forwarding and partly-forwarding actions	√	×	√	√	×	√	√	√	√	+ Studying the selfish behavior of a wide class of routing protocols - The selfishness model is weak
	Hui *et al.* [59]	Studying the different distributions of human altruistic models	√	√	×	√	×	×	√	×	×	+ Analyzing different altruistic behavior and message traffic models - Data delivery ratio analysis only
	Kouyoumdjieva and Karlsson [62]	Studying the effects of selfishness on publish/subscribe dissemination	√	×	×	√	×	√	×	×	√	+ Introducing energy-aware selfishness - The lack of design properties
	Bermejo *et al.* [83]	Studying the impact of battery level and social ties on routing performance	√	√	×	√	√	√	√	×	×	+ Applying real-world scenarios and applications in the experiment - Size-dependent performance analysis
	Xia *et al.* [84]	A signaling game to analyze the impact of uncertain data forwarding on routing	√	√	√	√	√	×	√	×	√	+ Introducing a more realistic selfishness model - No consideration of device energy
	Wang *et al.* [85]	An approximation method based on mean field game to study data diffusion	×	√	√	×	√	×	√	×	×	+ Comply with a philosophical saying for gossip diffusion in real social life - No analysis of diffusion delay
	Wang *et al.* [86]	A network formation game to analyze the opportunistic D2D offloading	√	×	×	√	×	×	√	×	×	+ Introducing the first selfish-aware D2D offloading model - No consideration of SS nodes
	Wang *et al.* [87]	A matching solution to analyze SS nodes on community-based D2D communications	×	√	×	√	×	×	√	×	×	+ The first work to analyze SS nodes in D2D communications - No evaluation of other metrics
	Cao *et al.* [88]	Analyzing node selfishness in the BS-to-device and D2D communications	√	√	×	√	×	×	√	×	×	+ Considering both IS and SS nodes - Requires all the link information to establish the time-varying graph
Hybrid	Ip *et al.* [63]	An ODE model to analyze probabilistic selfish behavior	√	×	√	√	√	×	√	√	×	+ Considering nodes with different transmission ranges - No analysis of social properties
	Li *et al.* [89]	A 3D-CTMC to model the message multicasting	√	√	√	×	√	×	√	√	×	+ Considers both IS and SS nodes - The network model is not general
	Wu *et al.* [90]	An ODE model to study the impact of IS and SS nodes on routing	√	√	×	√	×	√	√	√	×	+ Validating the theoretical results using simulations -Unrealistic routing assumptions
	Sermpezis and Spyropoulos [91]	A generic model to analysis the influence of SS nodes on routing based on mobility	×	√	√	√	√	√	√	√	√	+ Analyzing social selfishness policies - The nodes' social ties are identified based on only contact history
	Sermpezis and Spyropoulos [92]	An asymptotic model to analyze the impact of SS nodes on the performance of stateless routing	×	√	√	×	×	×	√	√	√	+ Analyzing delivery delay in heterogeneous networking scenarios - Data delivery delay analysis only

("√" if the protocol satisfies the property, "×" if not)

process and then conduct simulations to validate the theoretical results. Manam *et al.* [63] apply ordinary differential equation (ODE) model to analyze the impact of selfish nodes with probabilistic non-forwarding and non-copying actions and egotistic nodes (*i.e.,* nodes with different communication ranges) on the performance of the Epidemic and Two-hop protocols.

The numerical and simulation-based results in the presence of 50% of selfish and 50% egotistic nodes show that the delivery ratio goes up, the delay decreases, and the cost increases as the number of nodes increases from 0 to 70.

Unlike [63] that only addresses IS nodes, Li *et al.* [89] employ a 3D-CTMC model to evaluate the impact of the IS and SS nodes on the performance of Two-hop multicast in DTNs. To model the social selfishness, the network is divided into three non-overlapping communities V_1, V_2, and V_3, based on which the source and multicast destination nodes are placed in V_1 and V_3 and the IS nodes are placed in V_2. The numerical results show that the data delivery delay increases as the number of IS nodes increases. Additionally, it is concluded that the non-copying action of SS nodes affects the data delivery performance considerably. Wu *et al.* [90] apply the ODE model to evaluate the influence of IS and SS nodes on the performance of community-based DTNs using the Epidemic and Two-hop protocols. It is assumed that the network is divided into multiple communities where IS nodes do not relay messages to other nodes in the same community, whereas SS nodes relay messages to nodes in the same community. The experimental results demonstrate that the data delivery ratio decreases as the number of communities increases.

Sermpezis and Spyropoulos [91] study the impact of SS nodes on opportunistic data delivery performance by modeling different cooperation policies where the cooperation level of SS nodes is identified based on their contact rates. First, closed-form expressions are derived to approximate the expected data delivery delay with respect to a broad range of mobility scenarios. Next, simulations are conducted to validate the theoretical results using the synthetic and realistic mobility traces. The numerical results demonstrate that complex selfishness policies cannot achieve better performance than a uniform policy for power versus delay tradeoffs, whereas they can optimize power versus delivery ratio tradeoffs. Sermpezis and Spyropoulos [92] investigate the impact of SS nodes on the delivery delay in the Epidemic, Two-hop, and SnW protocols with heterogeneous contact distributions. The analytical expressions prove that a first-order mean value approximation for the basic epidemic spreading step becomes exact in large-scale networks.

Summary: Table I summarizes the important features of the research we studied in this section. It can be seen that a limited number of analytical techniques and tools (such as CTMC and ODE models) are employed to study the impact of human selfish behavior on the performance of data delivery protocols in WRNs, in comparison to other fields, such as opportunistic scheduling in opportunistic communication [93]. Meanwhile, almost all of the existing studies explore the data delivery delay and transmission cost parameters and do not study the other important parameters, such as the delivery ratio and energy consumption. In addition, there is a lack of an analytical technique to quantify the impact of human selfish behavior on D2D communications. Furthermore, despite the fact that a considerable number of simulation-based experiments study the human non-cooperative behavior in DTNs, the impact of human behavior in terms of different parameters (*e.g.,* delivery delay, transmission cost, and energy consumption) are not explored in D2D communications sufficiently.

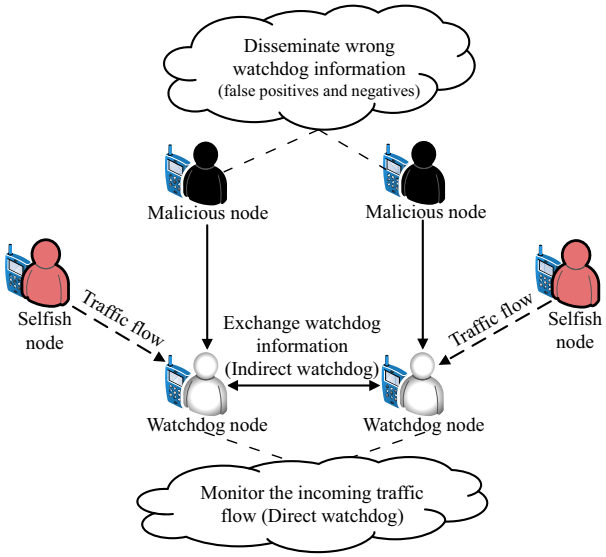

Fig. 7. A general watchdog scenario in non-cooperative WRNs.

IV. Selfish and Malicious Node Detection and Isolation Mechanisms

Detecting non-cooperative nodes and disseminating the detection information through the network can reduce the loss of network resources. Nevertheless, designing an effective detection and defense system in WRNs is extremely challenging due to the intermittent node connectivity and dynamic network topology. In other words, the misbehaving actions of selfish and malicious nodes are spread in space and time, and the observations of one node might not sufficiently indicate the misbehavior of its encountered nodes. This issue becomes more challenging when attackers collude with each other to boost their metrics and deceive the detection system. In the rest of this section, we discuss well-known selfish and misbehavior detection and defense systems in WRNs.

A. Selfish Node Detection Systems

We categorize selfish node detection schemes into two classes: watchdog systems and social trust-based communications. In the rest of this subsection, we introduce well-known works in each category and discuss their properties.

1) Watchdog Systems: as shown in Fig. 7, trusted watchdog nodes in watchdog systems analyze the traffic received from their encountered nodes to decide whether they have selfish behavior in message relaying or not (direct watchdog). However, inter-contact times (*i.e.,* two consecutive contacts) between nodes in WRNs can be quite long. Hence, the watchdog nodes may not receive sufficient direct watchdog information to judge the behavior of other nodes. Thus, they can share their opinions about other nodes with each other that help them detect the selfish nodes swiftly and accurately (indirect watchdog). When a node is detected as a non-cooperative node, it is called a *positive detection* (or positive); otherwise, it

is called *negative detection* (or negative). However, due mainly to the wrong watchdog information disseminated by malicious nodes, a watchdog node may detect a cooperative node as non-cooperative (false positive) or a non-cooperative node as cooperative (false negative) that can degrade the performance of the watchdog system severely.

Although several watchdog systems have been designed for wireless ad hoc networks (*e.g.,* [94] and [95]), they cannot be applied to WRNs due to their unique characteristics. A major reason is that the sender of a message in ad hoc networks can observe the relaying behavior of nodes in the delivery path of the message due to the end-to-end node connectivity. Thus, the sender node can detect the nodes' selfish behavior by analyzing the traffic on the message delivery path. In contrast, the observation of a node in WRNs may not indicate the selfish behavior of other nodes due to the intermittent node connectivity. Therefore, the node has to investigate the consistency of the history of contact and message exchange records (observed directly or received from other nodes) to detect selfish message droppers.

Recently, a number of cooperative watchdog systems have been proposed in DTNs. Hernández-Orallo *et al.* [96] propose a contact history-based collaborative watchdog scheme in which the watchdog nodes use both the direct and indirect watchdog information to detect selfish nodes. To reduce the impact of false positives and negatives, a controlled mixed diffusion method is applied where the positive detections are always diffused but a fraction of the negative detections is disseminated. Additionally, a 2D-CTMC model is designed to evaluate the detection time and ratio. The experiments show that the proposed scheme reduces the detection time from 20% for a very low degree of collaboration to 99% for higher degrees of collaboration. The extension of [96] is CoCoWa [97] in which a reputation scheme is designed to protect the watchdog system against the wrong watchdog information generated by malicious nodes.

Ayday and Fekri [98] propose a graph-based iterative algorithm, namely ITRM, to detect and isolate message droppers in DTNs. In ITRM, watchdog nodes store a rating table about the reputation of other nodes, which is updated based on their direct and indirect watchdog information. The rating table is represented by a bipartite graph where a check vertex shows a watchdog node, and bit vertices show all the nodes that the watchdog node has received watchdog information from them. When two nodes contact each other, they exchange a receipt for each received message along with a signed timestamp, based on which the watchdog nodes can detect message droppers. However, ITRM uses a binary reputation where the reputation (*i.e.,* type) of nodes can change easily if contradictory watchdog information is received. Similarly, Dias *et al.* [99] propose a reputation-based cooperative watchdog system to detect message droppers in which the reputation of nodes is updated based on their relayed and delivered messages. In addition, encountered nodes share their opinions about other nodes with each other to improve the detection performance. Finally, selfish and cooperative nodes are punished or rewarded, respectively.

Zhu *et al.* [100] propose a probabilistic detection scheme, namely iTrust, where a trusted authority (TA) checks the behavior of nodes based on their forwarding history evidence. To achieve a trade-off between the detection accuracy and cost, a reputation system is designed in iTrust where nodes with a good reputation are checked with a low frequency while suspicious nodes are checked with a high frequency. Moreover, an inspection game is played between an inspector (*i.e.,* TA) and an inspectee to find an optimal investigation probability and ensure that message droppers can be detected with a high accuracy and low communication overhead.

2) Social Trust-Based Systems: establishing social trust relationships between mobile nodes by leveraging their online social information (explicit trust) as well as their interactions or mobility properties (implicit trust) can help select trusted and secured relay nodes, thus improve the data delivery in WRNs [101]. In other words, social trust-based data relaying can avoid selfish nodes, thus stimulating them to cooperative in data forwarding [102]. In addition, it can protect the network against social trust-related malicious attacks, which will be discussed in Section IV-B5. However, establishing trust relations and propagating them in infrastructure-less wireless networks are very challenging because there is no centralized authority. In this subsection, we introduce well-known social trust management mechanisms in non-cooperative WRNs and discuss their properties.

IRONMAN [103] is one of the first social trust-based routing mechanism in which the nodes initially assign the highest trust value to their social friends. Then, encountered nodes exchange the history of their sent and received messages with each other, based on which they decrease the trust level of each other for each detected dropping message. Besides, a node increases the trust level of its encountered node when it receives a relaying message from that node. Additionally, the encountered nodes exchange their opinion about the trust level of other nodes with each other. However, IRONMAN initially assigns the highest trust score to each node, and thus selfish nodes have a chance to only forward their messages selfishly until their reputation is higher than a threshold value. To deal with this problem, in SENSE [104], nodes' social features, battery level, and message hop count are used to identify their altruism. Next, two encountered nodes agree to calculate the reputation of each other if their battery level is above a threshold value. Then, if the nodes deduce that they are non-selfish to each other, they exchange the history of their sent and received messages as well as their opinion about the reputation of other nodes with each other to faster detect selfish nodes.

Chen *et al.* [105] propose a dynamic social trust management mechanism to secure and optimize DTN routing in which the combination of quality-of-service (QoS) trust and social trust are used to select trustworthy relay nodes. While the delivery probability is considered to measure the QoS trust, healthiness and unselfishness metrics are introduced to measure the nodes' social trust level. When two nodes contact each other, they calculate the trust value of each other based on their direct contact and indirect trust information. The experiments using a stochastic Petri Net

TABLE II
SUMMARY OF THE SELFISH NODE DETECTION AND ISOLATION MECHANISMS IN WIRELESS RELAY NETWORKS

Detection method	Reference	Principle of proposed solutions	Influence analyze			Protection information			Fully distributed	Specialties (+) and limitations (-)
			Misreport	False positive	False negative	Contact records	Message records	Social features		
Watchdog Systems	Hernández-Orallo *et al.* [96]	A 2D-CTMC model to evaluate the selfish node detection time and overhead	×	√	√	√	√	×	√	+ Evaluation of the effects of false positives and negatives on detection performance - No consideration of malicious behavior
	Hernández-Orallo *et al.* [97]	A 4D-CTMC model to detect selfish nodes and cope with malicious nodes	√	√	√	√	√	×	√	+ Combines the collaboration with reputation - No consideration of social behavior
	Ayday and Fekri [98]	A graph-based iterative algorithm to detect malicious nodes	√	×	×	√	×	×	√	+ Combines QoS trust and reputation - No evaluation of the nodes' selfish behavior
	Dias *et al.* [99]	A cooperative selfish node detection mechanism based on node reputation	×	×	×	√	×	×	√	+ Realistic evaluation scenarios - No evaluation of false positives and negatives
	Zhu *et al.* [100]	A probabilistic misbehavior detection scheme based on inspection game	√	√	√	√	√	×	×	+ Achieves a high detection ratio with low communication overhead - Depends on a centralized third party
Social Trust-based Systems	Bigwood and Henderson [103]	A trust mechanism based on the self-reported social networks to detect selfish nodes	×	√	×	√	√	√	√	+ A simple benchmark detection method - Selfish nodes have chance to only forward their own messages before being detected
	Ciobanu *et al.* [104]	A social and content-based selfish node detection scheme	×	×	×	√	×	√	√	+ Considers both individual and social aspects of human altruism - Considers a binary social tie relation
	Chen *et al.* [105]	A social trust management scheme to minimize trust bias and maximize the routing performance	√	√	√	√	√	√	√	+ Deals with both selfish behavior and trust-related attacks - Lack of analytical evaluations
	Yao *et al.* [68]	A trust mechanism based on the social similarity to select trustworthy relay nodes	√	×	×	√	×	√	√	+ Exploits nodes' contact history and social features to identify their trust relationships - No evaluation of false positives and negatives
	Chen *et al.* [69]	An adaptive trust management mechanism for social IoT systems	√	×	×	√	×	√	√	+ Tunes the best trust parameters in response to changing the system conditions - Lack of analytical evaluations
	Ometov *et al.* [67]	A coalitional game approach to cluster nodes based on their trust level	×	×	×	×	×	√	×	+ Discussing several possible future research directions - No consideration of trust-related attacks
	Chen *et al.* [106]	A coalitional game to establish trusted D2D communications based on social ties	×	×	×	√	×	√	×	+ Considers both social trust and social reciprocity in relay selection - Only considers in-band communications
	Militano *et al.* [107]	A coalitional game for multi-hop content offloading in network-assisted D2D communications	×	×	×	√	×	√	×	+ The combination of social relationships and reputation to identify nodes' trust level - No consideration of trust-related attacks
	Zhang *et al.* [108]	A stoping theory to choose trusted relay nodes in D2D communications based on their physical and social information	×	×	×	√	×	√	×	+ An effective model to update nodes' reputation and detect their selfishness - Privacy concerns because of revealing the nodes' location information
	Yan *et al.* [109]	A rough set algorithm to select trustworthy relay nodes based on multi-dimensional trust relationships	×	×	×	√	√	√	×	+ The psychological structure of users are considered - No consideration of trust-related attacks
	Cao *et al.* [110]	A group-based video multicast system based on social trust and reciprocity in D2D communications	×	×	×	×	×	√	√	+ Employing real-world video traces

("√" if the protocol satisfies the property, "×" if not)

technique demonstrate that this method outperforms some existing trust-based and non-trust-based DTN routing protocols in terms of data delivery and delay. Similarly, trust routing based on social similarity (TRSS) [68] incorporates the concept of social trust into DTN routing where the nodes' common interests and social similarities are used to quantify their trust level. Next, nodes with higher social trust levels are selected as the message relays. Chen *et al.* [69] use the concept of honesty, cooperativeness, and community-interest to establish social trust relations between nodes, based on which a social-aware application can adjust the best trust-related parameters not only for establishing

secure communications but also maximizing the network performance.

While the studies above focus on DTNs, a number of recent studies have investigated the role of social trust in D2D communications. Ometov *et al.* [67] explore how the combination of human social-awareness and D2D communications can improve the communications performance and service quality. In particular, they propose a social-aware trusted D2D data delivery framework in which a coalitional game approach is employed to cluster mobile nodes based on their social tie strength and the degree of proximity. The evaluation results demonstrate that the proposed framework outperforms traditional cellular-only and network-assisted D2D communications in terms of energy efficiency and degree of connectivity. Similarly, Chen *et al.* [106] propose a coalitional game model to establish efficient and secure D2D cooperative communications by leveraging social trust and social reciprocity. The experiments show that this approach achieves up to 122% performance gain in comparison with the cellular-only communications. Similar coalition formation solutions are proposed in [107] and [110] to establish social trust-based network-assisted D2D communications.

In addition to the coalition formation methods discussed above, some other solutions have been proposed to select trustworthy relay nodes in D2D communications. Zhang *et al.* [108] propose a stopping theory to identify effective and trustworthy relay nodes in D2D communications wherein the nodes' social and physical information is captured to establish social trust relations among them. The experiments demonstrate that the proposed scheme achieves up to 120% and 45% performance gain over the case without D2D cooperation and random relay selection, respectively. Yan *et al.* [109] propose a trust-oriented partner selection mechanism in D2D communications in which multi-dimensional trust relations between the sender and possible relay nodes is established by evaluating their cognition, emotion, and behavior trust. Next, a rough set decision-making algorithm is designed to choose the most reliable relay node.

Summary: Table II summarizes the important characteristics of the watchdog and social trust-based systems in WRNs. It can be seen that almost all the watchdog systems rely on nodes' contact history, while the impact of the nodes' social relationships and preferences on the efficiency and effectiveness of watchdog systems are not explored sufficiently. In contrast to the watchdog mechanisms, the social trust-based systems exploit nodes' contact history and social relationships to choose more reliable and trustable relay nodes in message forwarding. Comparatively, most of the social trust-based systems in DTNs are fully distributed, whereas the social trust-based systems in D2D communications mainly take advantages of the underlying cellular network to establish the trust relationships between nodes and isolate selfish nodes. Besides, the majority of the social trust-based systems in DTNs analyze the impact of nodes' malicious behavior (*e.g.,* disseminating false positives and false negatives) on the performance of selfish node detection. While, the social trust-based systems in D2D communications cannot protect the network against malicious nodes' misreporting or other trust-related attacks.

B. Malicious Node Attack Detection Mechanisms

In Section II-E, we introduced different types of attacks that can be launched by malicious nodes in WRNs. In this subsection, we discuss well-known attack detection mechanisms.

1) Blackhole and Greyhole Detection Methods: Blackhole and greyhole are two common node attacks where an adversary drops all or a fraction of its relaying messages but forges its routing metrics to hide its malicious behavior. Although various blackhole and greyhole attack detection countermeasures have been proposed in wireless ad hoc networks (*e.g.,* [94] and [111]), they rely on end-to-end node connectivity that may not be applicable to WRNs.

Blackhole and greyhole detection mechanisms in WRNs primarily investigate the consistency of nodes' contact history and message exchange records to secure their communications and prevent the attackers from distributing falsified connectivity metrics. Li *et al.* [112] use encounter tickets to detect blackhole attackers in which two nodes sign an encounter ticket using their trusted private key identification when they contact each other. Accordingly, encountered nodes are required to submit their encounter tickets to their next encounters that prevent the attackers from claiming non-existing encounters. However, an adversary can still launch advanced types of the blackhole attack, such as tailgating wherein a node deliberately increases its contact frequency with popular nodes to attract more messages. To combat such attacks, a ticket-based prediction technique is designed in which a node predicts the competency of its encountered node to decide whether to forward a message to it or not.

While [112] investigates the contact history of nodes to detect blackhole attackers in DTNs, Dini and Duca [113] propose a reputation system where selfish nodes disseminate reputation value 0 to never be chosen as a relay node, whereas misbehaving nodes disseminate reputation value 1 to attract more messages. When a node receives a message, it updates the reputation of all nodes that the message relayed throughout. To cope with misbehaving nodes, a survival model is used in which a node periodically decreases the reputation of other nodes if it does not receive a message from them within a time period. In addition, Li and Cao [114] propose a detection system wherein a node is required to share the list of its sent and received messages with its next encountered node to help them judge whether this node has dropped any message or not. However, malicious nodes may manipulate their contact records to avoid being detected. To deal with this problem, a node is required to share a part of its contact records with other nodes, based on which the nodes can analyze the consistency of contact records received from different nodes and detect misreporting attackers.

While the methods discussed above can only detect blackhole attackers, Alajeely *et al.* [115] introduce a new type of greyhole attack called Catabolism attack in which adversary nodes drop some received messages and inject new fake messages instead. To deal with this attack, a defense

mechanism called Anabolism is proposed where a hash chain model is applied to detect the malicious nodes. Furthermore, Pham and Yeo [116] propose a statistical defense scheme, namely SDBG, to detect both individual and colluding black-hole and greyhole attackers. To detect the individual attackers, encountered nodes are required to exchange their contact history that let the other nodes judge their behavior. In particular, some sort of forwarding ratio metrics are designed in SDBG that help a judging node to compare the routing behavior of a judged node against threshold values. If the judged node is detected as an individual attacker, SDBG starts detecting possible colluding attackers in two phases. In the first phase, judging node identifies the potential colluders with the judged node based on the number of their received messages from the judged node. In the second phase, the judging node uses the forwarding ratio metrics to investigate the number of messages the judged node has forward to the suspicions colluders. The simulation results illustrate that SDBG outperforms the method in [114] with a detection rate of at least 70%.

Saha *et al.* [117] discuss that exchanging table-based information between nodes can cause high communication cost and long detection time. Thus, they use special trusted nodes (TNs) with long-range connectivity over the SnW protocol to detect malicious nodes by addressing the questions what information should be exchanged between TNs and how often. To this aim, they consider three scenarios: (1) TNs only exchange their contact information; (2) TNs exchange the information of malicious nodes; and (3) TNs exchange the information of malicious nodes along with additional information. The experimental results demonstrate that scenario 2 reduces the detection time by 26%, cost by 6%, and the detection ratio by 15-25% as compared to scenario 1. In addition, scenario 3 reduces the detection time by 45% and the detection ratio by 10% with a slight increase in cost as compared to scenario 2.

2) Data Flooding Attack Detection Methods: The primary goal of a flood attacker is to generate as many messages as possible to congest the network and waste the resources of other nodes. While several studies have attempted to alleviate the flood attack in wireless ad hoc networks [118] and peer-to-peer networks [119], they cannot be applied to WRNs because they require a permanent centralized monitoring server or end-to-end path information.

Recently, a number of studies have addressed the data flooding attack in WRNs. Li *et al.* [120] study the impact of flood attack on the performance of single-copy and multi-copy DTN routing protocols and show that the data flooding attack can waste more than 80% of the transmissions generated by honest nodes in the presence of 5% of flooding attackers. To deal with the flood attackers, a rate-limiting method is proposed in which a node can replicate a limited number of message copies. However, counting all the number of messages generated by a particular node may not be possible in WRNs because of the lack of a centralized center. Hence, a claim-carry-and-check method is adopted where each node claims the number of its generated or replicated messages to other nodes. Thus, the other nodes can cross-check their carried claims to detect inconsistent claims. Diep and Yeo [121] propose an encounter-based mechanism to detect flooding attackers without imposing strict limitations on nodes' message generation rate. In particular, a burst-limit policy is applied to restrict the flooding attack where the nodes' normal message generation pattern is still controlled using a rate-limiting method, but they are still allowed to have a small and short burst of new messages. To this aim, encountered nodes are required to exchange the list of their send and received messages with each other that can help them judge if another node violates the burst-limit policy.

While the above-mentioned studies rely on nodes' contact history, Parris and Henderson [122] propose a social-based defense mechanism against flooding attackers wherein each node is required to sign its forwarding messages and attach the list of its friends in each message. Thus, the trusted social friends of the source node only can carry its messages. Nevertheless, an attacker may spoof the header of a message to falsely make its encountered node believes that it is relaying its friend's message. In a worse case, the attacker may spoof multiple MAC-layer addresses to replicate a huge number of messages to a particular node. To deal with these attacks, a key distribution mechanism is designed in which a message is discarded if it is not truly signed by a friend.

3) Wormhole Attack Detection Methods: A wormhole attacker receives messages at one location of the network and then tunnels and retransfers all or some of them to nodes at another location in the network. In this way, the wormhole attacker can disturb and manipulate the topology views of the network. While several recent studies have addressed the wormhole attack in traditional wireless ad hoc networks (*e.g.,* [123]), a limited number of works have addressed the wormhole attack in WRNs. Ren *et al.* [124] propose a geographical-based mechanism where the node mobility is utilized to detect a forbidden topology. In this method, mobile nodes reduce their transmission range for short time and then the nodes' geometric relations are analyzed to detect wormhole attacks. The evaluation results demonstrate that the detection ratio goes up as the network density increases. Furthermore, it is found that the detection ratio increases when nodes have higher mobility. Pham and Yeo [125] propose a statistical-based approach in which infrastructure-based nodes collect and analyze the contact information of mobile normal nodes to detect and localize wormhole attackers. The detection process includes two phases: training and test. In the training phase, the average number of contacts between nodes over a period of time is calculated. Next, the testing phase checks if the ratio between the current node contacts and the mean contact number exceeds a threshold value.

4) Sybil Attack Detection Methods: A Sybil attacker (or Sybil) generates a large number of bogus identities or location information to establish many fake links in the network. Several detection techniques have been proposed for wireless networks that primarily use social network information (*e.g.,* [126]) or cryptography techniques (*e.g.,* [127]) to detect Sybil attackers [39]. Nevertheless, detecting Sybils and establishing a global trust in WRNs entails major challenges due to various reasons, such as the poor knowledge of nodes about the network's global state.

TABLE III
SUMMARY OF THE ATTACK DETECTION MECHANISMS IN WIRELESS RELAY NETWORKS

Attack model	Reference	Principle of proposed solutions	Attack model		Detection information				Fully distributed	Specialties (+) and limitations (-)
			Individual	Colluding	Contact records	Message records	Social features	Cryptography		
Blackhole and Greyhole Attacks	Li *et al.* [112]	A contact ticket-based scheme to detect message droppers	√	×	√	×	×	√	√	+ Predicts the node competency based on a belief system - No consideration of colluding attacks
	Dini and Duca [113]	The integration of reputation and probabilistic routing to detect attackers	√	×	×	√	×	√	√	+ Designs an aging method to determine the nodes' reputation - The lack of analytical evaluations
	Li and Cao [114]	A method that checks the consistency of contact records to detect message droppers	√	√	√	√	×	√	√	+ Can detect colluding misreporting nodes - No evaluation of false positives and negatives
	Alajeely *et al.* [115]	A hash chain model to detect nodes that drop messages or inject fake messages	√	×	×	√	×	×	√	+ Introduces a new attack model - Weak simulation settings
	Pham and Yeo [116]	A statistical method to detect individual and colluding droppers	√	√	√	√	×	√	√	+ Considers different contact manipulation models
	Saha *et al.* [117]	A lightweight detection scheme based on some trusted nodes	√	×	√	×	×	√	×	+ Achieves a better trade-off between the detection time and overhead - relies on long-range wireless connections
Flooding Attack	Li *et al.* [120]	A rate-limiting method to detect inconsistent node claims about the number of replicated messages	√	√	√	√	×	√	√	+ Less communication, computation, and storage costs - No comparison with previous work
	Diep and Yeo [121]	A rate-limiting method to detect flooding attacks that allows legitimate burst traffic	√	×	√	√	×	√	√	+ Can detect the burst traffic violation - The lack of analytical evaluations
	Parris and Henderson [122]	A social-based authentication system to detect flooding attacks	√	×	√	√	√	√	√	+ Considers various attack models - Evaluation with only one attacker
Wormhole	Ren *et al.* [124]	A geographical method to exploit the presence of a forbidden topology	√	√	×	×	×	×	√	+ A fully distributed detection method - Detection needs at least three nodes
	Pham and Yeo [125]	A statistical analysis method to detect and localize wormhole attackers	√	√	√	×	×	×	×	+ Detection mechanism does not rely on the number of nodes - relies on infrastructure nodes
Sybil Attack	Trifunovic *et al.* [128]	Study various types of Sybil attacks and evaluating their effectiveness	√	×	√	×	√	×	√	+ The valuation of four benchmark Sybil defence systems - No consideration of colluding attackers
	Liang *et al.* [129]	A trustworthy Sybil-resisted system to detect the service review attacks	√	√	√	×	√	√	√	+ Resists the review attacks without relying on a third authority
	Sun *et al.* [130]	A security mechanism against attackers that report forged virtual locations	√	×	×	×	×	√	×	+ measures metrics in client side but removes Sybils on the server side - No evaluation results
	Quercia and Hailes [131]	A social-based Sybil detection mechanism based on node ranking	√	×	×	×	√	√	√	+ Applying different ranking techniques - The possible wrong detection of an honest node as a Sybil
	Chang *et al.* [132]	A gateway-breaking algorithm to remove suspicious attack edges with high centrality	√	×	×	×	√	×	×	+ Each node carries small social profiles - relies on a centralized server
	Zhang *et al.* [133]	A social-based detection method based on nodes' abnormal contacts and pseudonym unstable behaviors	√	√	√	×	√	√	×	+ Detection of colluding Sybils - relies on a server to store nodes' contact information
Trust-related Attack	Chen *et al.* [105]	A dynamic trust management mechanism that is resilient against major trust attacks	√	√	√	×	√	×	√	+ An application-level trust optimization technique to discard less trustworthy recommendations
	Chen *et al.* [69]	An adaptive social trust mechanism that deals with several trust-related attacks	√	√	√	×	√	×	√	+ Resilience against attacks even in extremely hostile environments - No comparison with relevant methods
	Yao *et al.* [68]	A secure routing protocol that tolerates different trust-related attacks	√	√	√	×	√	×	√	+ Provides incentives for malicious nodes - no detailed descriptions about protecting against trust-related attacks

("√" if the protocol satisfies the property, "×" if not)

In general, Sybil detection methods in WRNs explore nodes' mobility and spatiotemporal information to detect Sybil attacks. Trifunovic and Hossmann-Picu [128] consider a case where a Sybil intentionally encounters its targeted nodes to enhance its contact frequency and strengthen the weight of its social relationships with them. The experiments demonstrate

that implementing successful Sybil attacks using mobility is costly for a mobile Sybil because it needs to invest several hours to infiltrate a community successfully. Liang *et al.* [129] propose a sybil-resisted trustworthy service evaluation system, called SrTSE, in which two types of Sybils can exist. First, users who put a bad review about a service provided by a vendor while it is good. Second, a vendor along with a group of users who put good reviews about a bad service to increase its reputation. To prevent these attacks, SrTSE assumes that a user can only put one review about a vendor in a short period of time. Thus, if a user puts several reviews with different pseudonyms about a vendor at a particular time, it will be considered as a Sybil. Sun *et al.* [130] propose a geographical mechanism to detect Sybils that report forged virtual locations. In particular, a two-dimensional coordination system is designed on the server side that obtains the set of Euclidean distances between nodes and generates a set of candidate nodes for routing. In case a Sybil node forges an unreal location, a high dimensional location is generated as output inferring that the node is a Sybil node.

A couple of existing works exploit nodes' social network information to detect Sybil attacks. MobID [131] deals with Sybil attackers who may produce several fake identities but have a few real-life relationships. In MobID, a node enlists the identity of its encountered nodes in two small networks: the network of friends and network of foes. Thus, the node explores the social similarity between the friends and foes networks to decide whether an unknown contacting node launches a Sybil attack or not. Chang *et al.* [132] consider a community-based MSN where both Sybils and well-behaved nodes exist in the network. In addition, a local ranking system is employed to identify trust and distrust relations among nodes. Thus, a node stores two random social profiles: a trust profile and a distrust profile. When two strangers contact each other, they exchange their trust profile with each other to calculate the trust and distrust levels of each other, based on which they can decide whether another one is Sybil or not. Zhang *et al.* [133] introduce a social-based Sybil detection scheme in which contact patterns and pseudonym behavior of nodes are investigated to detect Sybils. Since the storage and computational capabilities of mobile devices are limited, cloud servers are utilized to process the nodes' contact traces and detect Sybils.

5) Social Trust-Related Attack Detection Methods: The social trust relationships between mobile nodes can be exploited to establish reliable and secure communications in WRNs. Nevertheless, malicious nodes falsify the trust level of their owns or their friends in order to attract more services or messages) but later refuse to provide the promised services. Besides, they can launch a colluding attack to spoil the good reputation of well-behaved nodes. In general, three major trust-related attacks in the context of WRNs have been considered in the literature: self-promoting attack where an adversary aims to promote its trust level, bad-mouthing attack in which an adversary ruins the trust level or reputation of other (well-behaved) nodes, and ballot-stuffing attacks wherein an adversary exaggerates the trust level of other malicious nodes. To deal with these attacks, Chen *et al.* [105] investigate the consistency of the encounter tickets received from different nodes based on a metric called healthiness social trust (that is the belief of a node whether another node is malicious or not) to identify the self-promoting attacks. Moreover, the consistency of trust recommendations provided by other nodes is checked to detect the bad-mouthing and ballot-stuffing attacks. Similarly, Yao *et al.* [68] and Chen *et al.* [69] check the consistency of nodes' direct and indirect trust recommendations to detect the trust-related attacks.

Summary: Table III summarizes the main features of the attack detection techniques. It can be seen that a few numbers of the blackhole and greyhole attack detection mechanisms (*i.e.,* [114] and [116]) can protect the network against colluding message droppers. In addition, nodes' social features and relationships are not considered in the existing blackhole and greyhole attack detection mechanisms. Besides, a limited number of data flooding and wormhole attack detection mechanisms are proposed in WRNs where only [122] uses nodes' social features to detect malicious attackers. In contrast, almost all the Sybil detection methods primarily take nodes' social relationships into account to detect Sybil attackers. Nevertheless, a few numbers of them (*e.g.,* [129] and [133]) can detect the colluding Sybil attackers. Furthermore, the trust-based attack detection mechanisms mainly apply nodes' contact and social information to identify both untrustworthy individual and colluding nodes. While almost all the attack detection schemes are designed for DTNs, detecting malicious nodes in D2D communications with respect to their specific characteristics needs further explorations.

V. Incentive Mechanisms

Mobile nodes may not be willing to share their resources with each other and participate in data relaying unless an appropriate incentive is provided. However, designing an effective and fair incentive mechanism in WRNs is extremely challenging because mobile nodes do not have complete information about the network's global state. Furthermore, nodes with different resource constraints and preferences may require different types of incentives to cooperate with each other in data delivery. The ultimate goal of an incentive scheme is to make the rewarding mechanism incentive-compatible implying that a node obtains the highest reward when it has honest behavior. Broadly, existing incentive mechanisms can be classified into three categories: tit-for-tat (TFT)-based, reputation-based, and credit-based schemes. In the rest of this section, we study well-known incentive schemes in each category and characterize their main features.

A. TFT-Based Incentive Mechanisms

The main idea in TFT-based mechanisms is to force nodes to exchange the same number of messages during an opportunistic contact. In other words, TFT-based mechanisms aim to ensure that mobile nodes provide better forwarding services for cooperative nodes but avoid selfish nodes. Shevade *et al.* [134] propose a TFT mechanism for DTNs in which the concepts of generosity and contrition are employed to respectively overcome bootstrapping (*i.e.,* who starts the cooperation) and exploitation (*i.e.,* when another node exploits) problems. In

this work, encountered nodes exchange their contact information periodically, based on which a source node can calculate the forwarding path of its messages. Finally, when a message is delivered to its destination, intermediate nodes in the delivery path are awarded. The simulation results show that the data delivery ratio increases up to 60% in comparison with a fully cooperative scenario. Similarly, Buttyán *et al.* [135] propose a barter-based approach where encountered nodes exchange the list of their messages with each other. Next, they identify candidate messages and their forwarding priorities. Finally, they exchange their messages one by one until all of them are processed or their connection is lost. However, the message exchange methods in [134] and [135] can cause deadlocks in case nodes do not have the same number of messages. Meanwhile, the value of messages is not considered in their incentive mechanism.

To deal with above-mentioned problems, MobiTrade [136] allows nodes to exchange messages if they do not have the same number of messages. In MobiTrade, the value of a message is identified based on the number of nodes that are interested in the message and nodes' cooperation degree. In addition, a buffer allocation technique is applied that helps a node to split its buffer for each channel based on its knowledge of future demand. Similarly, Zhou *et al.* [137] propose a TFT-based content dissemination scheme for publish-subscribe systems in which the order of forwarding messages is identified based on a content utility function. Specifically, the utility of a message for a certain node is identified based on the number of nodes interested in the message, node contact probability, and the cooperation level of nodes.

A number of recent studies employ the TFT approach to promote the cooperation of nodes in D2D communications. Hsu and Duan [138] propose an equal-reciprocal mechanism for data sharing in D2D communications where D2D nodes are grouped based on their physical information. Next, each node in a group can share the same number of content with each other. The experiments show that this method not only guarantees the fairness in content sharing but also maximizes the individual utility of the nodes. Additionally, D2D Fogging [139] is a collaborative task offloading and execution mechanism in which a set of TFT resource constraints and an energy budget constraint is introduced to stimulate over-exploited and free-rider nodes to participate in data sharing. The TFT resource constraints ensure that a node can utilize the resources of other nodes if it shares more resources with the others. Furthermore, Lyapunov optimization methods are developed to minimize the energy consumption of D2D nodes with respect to those incentive constraints. The simulations demonstrate that the energy consumption of nodes reduces by 30-40% in comparison to a case each node executes its tasks locally. Mastronarde *et al.* [140] employ an online supervised learning algorithm that helps a node learn its cooperation policy and make a decision whether to relay messages received from other nodes or not. The experimental results reveal that the network achieves the highest performance when there exist many nodes with high energy resources to relay messages.

B. Trust and Reputation-Based Incentive Mechanisms

In the trust and reputation-based incentives, mobile nodes assign appropriate reputation to each other based on their direct trust relationships or indirect trust recommendations provided by other nodes. Eventually, better services are provided for nodes with high reputation or strong trust relationships. Under these circumstances, the nodes are stimulated to relay messages received from other nodes to gain enough reputation so that they can get help from other nodes. However, identifying the actual reputation of nodes in WRNs is challenging because the nodes cannot observe the behavior of each other thoroughly. Meanwhile, malicious nodes can manipulate their reputation for pretending that they have participated in data delivery.

MobiGame [141] is a user-centric reputation system wherein a node submits the receipts of its relaying messages to the source and destination nodes to obtain credits. A message for an intermediate node can be a good bundle if the node can forward the message before it expires or a bad bundle if the message is close to being expired. It is assumed that both selfish and malicious nodes exist in the network where the selfish nodes do not return the relay evidence to the previous relay nodes. Meanwhile, the malicious nodes distribute bad bundles to other nodes to waste their resources. To establish a fair interaction, a game-theoretic model is designed in which the costs and utilities of forwarding and receiving good and bad bundles are analyzed using perfect Bayesian equilibrium. Similarly, IRONMAN [103] applies nodes' self-reported social network information to initialize their reputation. When two nodes A and B contact each other, they exchange their contact history, message-forwarding history, and the reputation of other nodes with each other that can help them update their opinions about the reputation of each other and other nodes. Once the reputation of one of them, say A, is less than a threshold value, B discards messages received from A until A improves its reputation by relaying messages received from other nodes.

While the reputation mechanisms proposed in [103] and [141] are fully distributed, MobiCoop [142] designs reputation-based incentives for hybrid DTNs in which nodes can contact each other through both service-oriented and opportunistic communications. Each node uses both direct and indirect observations to update the reputation of other nodes. In particular, three parameters including battery level, the Internet connectivity, and cooperation degree are used to calculate the reputation of a node. For example, the highest reputation value is awarded to a node that has a low battery level and access to the Internet, but it is still willing to cooperate with other nodes. However, MobiCoop depends on a centralized Web service that may not be available in distributed DTNs.

Summary: Table IV summarizes the main features of our studied TFT-based and reputation-based incentive mechanisms. It can be seen that the TFT mechanisms stimulate mobile nodes in both DTNs and D2D communications, whereas almost all the reputation-based schemes focus on promoting node cooperation in DTNs. Comparatively, TFT-based methods can work well when the network traffic is high,

TABLE IV
SUMMARY OF THE TIT-FOR-TAT AND REPUTATION-BASED INCENTIVE MECHANISMS

Model	Reference	Principle of proposed solutions	Incentive objective	Specialties (+) and limitations (-)
Tit-For-Tat	Shevade *et al.* [134]	An incentive mechanism that incorporates the generosity and contrition into the routing	Maximizing the individual utility of nodes	+ Extensive evaluations using both synthetic and real-world traces - No consideration of fairness
	Buttyn *et al.* [135]	A barter game model to promote node cooperation	A node can obtain a message if it gives a message in return	+ Considers the value of messages - Limited analytical results
	Krifa *et al.* [136]	A mechanism that allows nodes to trade its relaying messages and buy its interested messages	Maximizing the expected utility of each stored message for future encounters	+ Provides a customized resource allocation strategy for each node
	Zhou *et al.* [137]	A content-based incentive mechanism that stimulates nodes to transmit their messages to interested nodes in publish/subscribe systems	Maximizing the future trading value of a stored message	+ Selects forwarding messages based on their value and nodes' cooperation level - Applies a complex content matching in the message selection process
	Hsu and Duan [138]	An equal-reciprocal incentive mechanism for social group-based data sharing in D2D communications	Maximizing the utility of nodes, which is the amount of contents a node uploads minus those it downloads from the network	+ No need to compute nodes' sharing probabilities in advance - Caching capacity of nodes is not considered
	Pu *et al.* [139]	A cooperative task offloading and execution framework in D2D communications	A node can use the resources of other nodes if it shares more resources with the others	+ The framework is lightweight and operates dynamically according to the system's current information
	Mastronarde *et al.* [140]	A supervised learning algorithm that help nodes adapt their cooperation policy in D2D message relaying	Maximizing the utility of nodes, which is the difference between a node's message forwarding utility and energy consumption	+ Considers different mobility and relay budget classes
Reputation-based	Wei *et al.* [141]	A game-theoretic scheme to stimulate nodes and resist attacks	Maximizing the individual utility of nodes in message forwarding	+ Considers both security and fairness - Limited analytical and simulation results
	Bigwood and Henderson [103]	A social-based trust mechanism to identify node reputation	Maximizing the reputation of nodes based on their cooperation history	+ The establishment of trust relationships between the nodes using their social information - The lack of theoretical analysis
	Silva *et al.* [142]	A generalized system to stimulate cooperation in mobile applications	Maximizing the battery life of mobile devices	+ Using real application prototypes in the evaluations - Relies on a web service to manage the node reputation

but they cannot provide fairness if encountered nodes do not have the same number of messages to exchange. Meanwhile, the message selection process in TFT-based mechanisms can affect their effectiveness in terms of the message delivery ratio significantly. In contrast, the performance of reputation-based mechanisms highly depends on the direct observations of nodes and the distribution of recommended-based reputations [143].

C. Credit-Based Incentive Mechanisms

Credit-based incentive schemes employ different forms of virtual credit to reward the cooperative nodes where the rewarding is commonly managed by a third-party credit clearance center (CCC). The idea is that a node is rewarded credit for relaying messages received from other nodes or sharing its resources with them where it can later use its credit to pay other nodes for achieving its own utilities. In this way, selfish nodes are not rewarded if they do not relay messages for others, and thus they cannot afford to buy the forwarding service of other nodes.

Broadly, existing credit-based incentive mechanisms can be categorized into two classes: game-theoretic and security-based mechanisms. The game-theoretic schemes aim to establish a win-win credit assignment situation among interacting nodes, whereas the security-based methods attempt to ensure the security of credit. In addition, there are some miscellaneous credit-based mechanisms that do not fall in the game-theoretic and security-based mechanisms. In the following, we present well-known credit-based mechanisms in each category.

1) Game-Theoretic Credit Mechanisms: game-theoretic methods are widely applied to characterize the cooperations and competitions among rational mobile nodes with conflicting interests in wireless communications [144], [145]. For example, a BS can set constraints on the transmission parameters in D2D communications so that mobile nodes compete or cooperate with each other to reuse the radio resources efficiently. In general, a game in WRNs consists of a set of players (*i.e.,* mobile nodes and BSs), rules, strategies, and payoff (or utility) where each player chooses a strategy with the aim of maximizing its utility. The payoff is normally calculated based on the difference between the reward and cost of relaying a message (*e.g.,* resource consumptions). Assuming that mobile nodes are selfish and rational, a binding agreement or

equilibrium point should lead to a win-win situation where no player can improve its utility by unilaterally deviating from the equilibrium. In the rest of this subsection, we first study non-cooperative game-based credit schemes, followed by introducing the cooperative game-based credit schemes.

Stackelberg Game-based Credit Schemes: Stackelberg game is commonly played between a BS (*i.e.,* leader) and mobile nodes (*i.e.,* followers) in which the BS has an incentive to share a channel with some nodes if it is profitable. The BS decides the price, and the nodes choose the transmission power and channel given the charging price. The utility of the BS can be defined as its throughput plus the price it charges, whereas the utility of the nodes is the difference between its throughput and the cost that it pays to the BS for using the channel [146].

Sugiyama *et al.* [147] propose a two-stage Stackelberg game-based pricing scheme wherein a network operator decides how much it should pay to mobile nodes if they participate in data delivery. First, the operator announces the total reward and the minimum number of required participating nodes. Next, candidate nodes play the game to decide whether they want to cooperate in data forwarding or not. Finally, the operator shares the reward among the collaborative nodes if their number is higher than the required value. The cost of relaying a message by a node is identified based on its storage and energy consumptions, and their revenue is identified using a prospect theory. Finally, backward induction method is used to analyze the tradeoff between the cost and revenue and find the Nash equilibrium. Chen *et al.* [148] model the interactions between a BS and mobile nodes as a Stackelberg game in which the BS aims to minimize its rewarding cost, and mobile nodes aim to maximize their utility by choosing an appropriate caching decision. Particularly, an iterative gradient algorithm is applied to find the Stackelberg equilibrium and maximize the utility of both the BS and nodes. A similar Stackelberg game-based incentive scheme is proposed in [149].

Some existing credit-based mechanisms employ Stackelberg game to optimize quality-driven multimedia video sharing in WRNs. Wu and Ma [150] propose an incentive scheme for distributing video files in which an interested node (leader) publishes a request to receive a video file by declaring a total credit for the delivery. Next, all the participants (followers) compete with each other to deliver the video file and earn credit. Since each video frame could increase the quality of the reconstructed video file, the destination node measures the value of each video frame using a utility function and reward each participating node based on its total contributions. Wang *et al.* [151] and Wu *et al.* [152] employ Stackelberg game to design incentives for video sharing in network-assisted D2D communications in which the game is played between a multimedia content provider or BS as the leader and nodes with video contents as the followers (see Fig. 8). The objective is to maximize the benefits of the leader while stimulating the followers to participate in data sharing. Wang *et al.* [151] propose a Stackelberg game-based source selection and power control solution where higher power and price are assigned to important packets to increase their delivery probability. Thus, the BS decides which devices to select and how much to pay for their provided radio

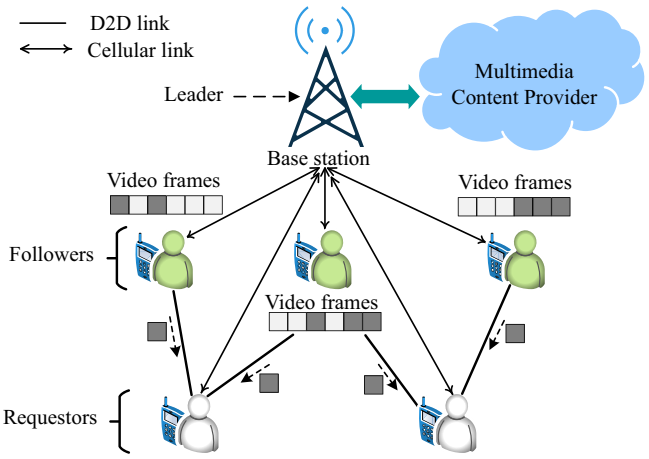

Fig. 8. An illustration of video content sharing via network-assisted D2D communication using Stackelberg game.

resource. To this aim, Stackelberg equilibrium is employed to efficiently allocate the optimal power to the selected devices. Wu *et al.* [152] employ nodes' social and mobility features to select appropriate relay nodes that can efficiently distribute the video contents to interested peers. Next, a Stackelberg game is played between the BS and selected nodes to maximize their utility.

Auction Game-based Credit Schemes: auction is a popular incentive mechanism for scenarios in which the value of a service or trading item is undetermined. In a typical auction, a seller first announces the auction, and buyers respond to the auction in terms of biding. Next, the seller identifies the result of the auction and assigns the resources to the winners. Xu *et al.* [153] propose a sequential second price auction to allocate spectrum resources in a network with a BS and multiple D2D devices where the spectrum resource units are auctioned off by D2D devices. In each round, the D2D devices offer a bid based on the value of the current resource unit, and then the BS allocates the unit to a device with the highest bit value but pays the second highest bid. The game continues until all the resource units are sold. The utility of a device is the difference between the total value of spectrum units obtained and the total payment. This work is extended in [154] where the game is played among a BS, cellular nodes, and D2D nodes. In particular, a reverse iterative combinatorial auction mechanism is modeled to efficiently allocate the spectrum resources and reduce the intra-cell interference wherein the buyers are motivated to offer multiple bids on combinations of resources iteratively and the seller asks the prices in each round. The experiments demonstrate that the system sum transmission rate increases as the number of D2D devices and resource units increases.

A major problem with the solutions in [153] and [154] is that D2D devices have to submit the game information (*e.g.,* prices and costs) in each round of the game, while one of them will receive the reward finally that wastes their energy. To deal with this problem, Huang *et al.* [155] propose a sequential posted pricing method in which the BS announces the auction by sending a posted price to the devices and assigns the

resource unit to only one owner in each round. In this way, the BS stops activating the rest of devices because there exists already an active owner accepting the offer. The experiments show that this method achieves a better tradeoff between the BS's cost and the number of active devices.

Hajiesmaili *et al.* [156] propose an auction-based incentive scheme for load balancing in D2D-enabled cellular networks where the main goal is to dynamically shift the portion of the traffic of heavily-loaded cells to other under-utilized cells. To this aim, an online procurement auction mechanism is proposed in which multiple devices submit bids, and the BS evaluates the bids and purchases a subset of the resource units to satisfy the load balancing requirement while minimizing the social cost. The experiments demonstrate that the proposed scheme achieves a near offline-optimal performance.

Bargaining Game-based Credit Schemes: bargaining is a cooperative game approach in which the main goal is to fairly divide a certain surplus or credit among game players through negotiation. In the context of WRNs, bargaining game-based credit schemes have been extensively employed to model message trading between encountered mobile nodes with respect to their different criteria and preferences. Ning *et al.* [157] consider a scenario in which mobile nodes willingly relay their interested messages but expect credit for relaying messages that they are interested. Since a credit is awarded only to the first deliverer and none of the nodes want to waste their resources, they design a two-player bargaining game where the encountered nodes negotiate over the value of their messages with respect to their delivery probability. Specifically, Nash bargaining equilibrium is employed to find an optimal solution, yielding the players exchange messages with the maximum gained credit. Similarly, self-interest-driven (SID) [158] proposes a two-player bargaining game for ad distribution wherein the players can trade both ad packets and virtual checks attached to each ad packet. In particular, the Nash bargaining equilibrium is applied to find a Pareto optimal point where both the players can reach a binding agreement. However, the rewarding mechanism in [157] and [158] are not fair because only the last-hop final deliverers are rewarded.

Wu *et al.* [159] propose a bargaining model to stimulate selfish nodes to cooperate in probabilistic routing protocols. The message trading is motivated by a marketing concept in which a message as a good is traded from a node with lower delivery probability to another node with a higher delivery probability. Thus, the current carrier of a message (seller) bargains with another node (buyer) over the value of the message in some rounds until an agreement on the price is reached, or they finally disagree. To identify the best strategy profile, a unique subgame perfect equilibrium is applied that helps the players to reach an agreement in the first round.

A number of bargaining schemes consider the sender of a message as a buyer who wants to buy the forwarding service of the receiver who is a seller. Li *et al.* [160] design a two-player bargaining game assuming that the buffer and energy level of nodes are limited. First, the buyer offers price *a* considering its free buffer, current wealth, and the message time-to-live (TTL). In contrast, the seller offers price *b* with respect to its resources and the wealth. Next, they either agree to trade the message with price $\frac{(a+b)}{2}$ if $a \geq b$ or disagree if $a < b$. Furthermore, a bidding function is designed in a way that the buyer offers a high price when it is rich. In addition, the seller offers a high price when its resources are limited and a lower price when it is poor and needs to guarantee the forwarding of its own messages. Similarly, Jedari *et al.* [161] propose an alternating-offers bargaining game, namely GISSO, in which the buyer and seller value the forwarding service based on their individual and social utilities where the utility of the messages is identified based on their social tie strength and message appraisal. Next, they negotiate over the service value in some rounds until they reach an agreement or the game is over. In GISSO, subgame perfect Nash equilibrium is applied to establish a win-win condition between the nodes where backward induction is employed to identify the best strategy for the players. Similar bargaining-based incentive schemes have been proposed in [162] and [163].

Coalition Formation Game-based Credit Schemes: coalition formation is a cooperative game approach in which a set of players (*e.g.,* mobile nodes) agree to act as a single entity to gain a higher payoff, which is called coalition value. Han and Poor [164] study data forwarding in DTNs by highlighting that nodes on the boundary of the network (boundary nodes) are not willing to cooperate with backbone nodes in data relaying. To deal with this problem, the concept of *core* is employed to establish stable coalitions in which the boundary and backbone nodes in a coalition have the incentive to cooperate with each other in data transmission. Next, they propose a routing protocol based on the coalition and repeated games, which improves the network connectivity by about 50%. Similarly, Akkarajitsakul *et al.* [165] design a coalitional game to stimulate the cooperation of selfish nodes wherein the nodes decide either join or leave a coalition based on their individual payoffs. The individual payoff of a node is identified based on the delivery delay of their messages received from the BS and the cost incurred by this node for relaying the messages to other nodes. Using a Markov chain model to evaluate the stability of the coalitions, the experiments demonstrate that the nodes achieve a non-zero payoff.

A couple of coalitional game-based incentive schemes aim to design efficient content distribution and resource allocation protocols in D2D communications. Zhang *et al.* [166] design a merge-and-split coalitional game with a transferable payoff (*i.e.,* utilities like money are allocated to the players in the coalition) to efficiently allocate the spectrum resources between D2D and cellular devices. The utility of the D2D and cellular devices is defined as the sum transmission rate they can achieve through the resource blocks allocated to them. Hence, the game is divided into several sub-games where each sub-game addresses the resource allocation problem of one resource block. Since the nodes aim to maximize their utility, they have an incentive to form a strong group and win their preferred spectrum resources. In contrast to [166], Zhu *et al.* [167] employ a non-transferable coalition formation game (*i.e.,* different players have different interpretations of utilities) for energy-aware content sharing through D2D communication. Similarly,

TABLE V
SUMMARY OF THE GAME-BASED CREDIT MECHANISMS

Game approach	Incentive objective	Analytical tools	Achieved performance
Stackelberg game Sugiyama *et al.* [147] Chen *et al.* [148] Yin *et al.* [149]	[149]-Attracting more nodes by the operator while minimize losing their energy and buffer [150]-Minimizing the cost of BS while maximizing the utility of nodes [151]-Maximizing the sum rates of D2D devices while guaranteeing the cellular nodes' data rate requirement	[149]-Backward induction [150]-Subgame perfect equilibrium [151]-Successive convex approximation	[149]-A win-win relationship between operators and mobile nodes [150]-The caching scheme is beneficial to D2D devices if their requested pattern is more heterogeneous [151]-Achieves high performance while reducing the overhead of cellular nodes
Auction game Xu *et al.* [153] Xu *et al.* [154] Huang *et al.* [155] Hajiesmaili *et al.* [156]	[155]-Maximizing the sum rate of the BS and the nodes' obtained resources while minimizing the nodes' payments [156]-Maximizing the network sum rate by allowing cellular nodes to share their resources [156]-Minimizing the overhead of the BS and the energy consumption of D2D devices [158]-Fulfilling load balancing requirement with the minimum social cost	[155]-Subgame perfect equilibrium [156]-Integer linear program [157]-Backward induction [158]-Mixed integer linear program	[155]-High performance on the system sum rate, efficiency, and fairness [156]-Superior to the random allocation, high system efficiency, and stable over different parameters of nodes and resources [157]-A better tradeoff between the BS's cost and the winning percentage of nodes [158]-Reduces the cost by 45% compared with an alternative heuristic
Bargaining game Ning *et al.* [157] Ning *et al.* [158] Wei *et al.* [159] Li *et al.* [160] Jedari *et al.* [161] Xu *et al.* [162] Li *et al.* [163]	[159]-Maximizing the reward of sender nodes [160]-Gaining a balanced credit while distributing as many ads as possible [161]-Earning higher credit balance [162]-Maximizing the node utility based on the buffer space and TTL [163]-Maximizing the node utility considering the message TTL, delivery delay, and social tie [164]-Maximizing the node utility based on the buffer, energy, and TTL [165]-Saving the forward capability of nodes to serve the fitness messages	[159][160][165]-Nash bargaining theorem [161][163][164]-Subgame perfect equilibrium	[160]-Reduces the transmission cost while maintaining a good delivery ratio and delay [161]-Up to 75.8% gain in data delivery in comparison with a non-incentive routing [162]-Reduces the buffer consumption while delivering messages before the expiration [163][164]-A good data delivery ratio and delay in the presence of selfish nodes [165]-Saves the network bandwidth and buffer while keeping a high delivery ratio
Coalition game Han *et al.* [164] Akkarajitsakul *et al.* [165] Zhang *et al.* [166] WZhu *et al.* [167] Cao *et al.* [109] Xiao *et al.* [168] Zhao and Song [169] Wang *et al.* [170]	[166]-Establishes stable coalitions in which backbone and boundary nodes fairly cooperative [167]-Maximizing the nodes' payoffs [168]-Nodes intend to maximize their utility, hence they have an incentive to form strong and stable coalitions [169]-Physically neighboring nodes form coalitions to minimize their energy consumption [111]-Maximizing the utility of spectrum sharing by stimulating nodes in a coalition to cooperate with each other [170]-Each node chooses a specific BS to maximize its transmit rate per bandwidth price [171]-Minimizing the power consumption of nodes while satisfying their power budget [172]-BS maximizes the system sum rate while D2D devices maximize their individual payoffs	[166]-Market fairness [167]-Markov chain model [168]-Max-coalition order [170]-Matching theory [171]-Coalitional graph game [172]-Defection function	[166]-The network connectivity is improved by about 50% [167]-Nodes achieve higher payoff comparing to a case they act alone [169]-All nodes participating in D2D content sharing achieve positive utilities [111]-Improves the nodes' perception quality of mobile video multicast effectively [170]-Improves the system performance, especially in a large coverage area with a large number of D2D devices [171]-Power consumption is almost optimal in a small-scale D2D network [172]-Improves the system performance up to 93% in compare to the case without community cooperation
Algorithmic game Cai *et al.* [171]	Maximizing the reward of only when they honestly report their encounter probability	Sequential stopping rule	Achieves higher data delivery ratio with low overhead
Evolutionary game El-Azouzi *et al.* [172] Lena Cota *et al.* [173] Wang *et al.* [174]	[174]-Maximizing the probability of success [175]-Tolerating node selfishness while achieving high system performance [176]-Maximizing sum of all nodes' utilities	Evolutionary game theory	[174]-Reaches the equilibrium point using the nodes' local estimations [175]-Improves the bandwidth overhead by 22% in a live streaming use case
Minority game Chahin *et al.* [175]	An optimal performance tradeoff between the delivery ratio and resource consumption	Nash equilibrium	Reaches the equilibrium point using the nodes' local estimations
Repeated game Huang *et al.* [176] Barua *et al.* [178]	[178]-Maximizing the payoffs of BSs as players, which are the payoffs from both cellular and D2D communications using radio resources [179]-Maximizing the utility of both BS and D2D devices in the presence of selfish nodes	[178]-Nash equilibrium derivations [179]-Nash equilibrium	[178]-Improves the system sum data rate and sum gain [179]-Maximizing the utility of the BS and D2D devices while resists selfish deviations
Mean filed game Li *et al.* [178]	Stimulate devices to truthfully reports the number of chunks they receive	Mean field equilibrium	Implementation on Android devices illustrates its efficient performance
Signaling game Zhang *et al.* [179]	Maximizing the monetary benefit of nodes while guaranteeing a non-zero payoff for the BS	Separating equilibrium	Improves the system sum transmission rate
Network formation game Wang *et al.* [86]	Maximizing the individual payoffs of nodes	Pairwise stability	The performance gap between selfish and selfless nodes becomes smaller as the communication cost of cellular and D2D transmissions increases

Xiao *et al.* [168] model a Bayesian overlapping coalition game with non-transferable payoffs for efficient spectrum resource allocation.

Some studies exploit nodes' social features to form strong coalitions in D2D communications. Cao *et al.* [110] and Wang *et al.* [170] employ nodes' social tie information

(*e.g.,* social trust and reciprocity) to form stable coalitions, based on which D2D devices are stimulated to share their resources with each other, and the BS can share the spectrum resources efficiently. Similarly, Zhao and Song [169] propose a coalition game-based incentive mechanism in D2D communications where the objective is to minimize the total power consumption while satisfying nodes' social incentive constraints.

Other Game-based Incentive Approaches: other types of game-based credit mechanisms have been proposed in DTNs. Cai *et al.* [171] incorporate algorithmic game theory into the Two-hop protocol where a sequential stopping rule is employed to select the best relay nodes with maximum reward. Next, a second-price auction game is applied to identify the reward value in which a relay node can get the maximum reward if it reports its routing metrics honestly. Once a message is delivered to its destination, the source node rewards the intermediate nodes in the delivery path. El-Azouzi *et al.* [172] employ an evolutionary game to promote the cooperation of nodes in the Two-hop protocol. Similarly, Wang *et al.* propose a simple but effective incentive approach based on evolutionary game theory in community-based opportunistic networks wherein nodes voluntarily participate in message relaying and punish other non-cooperative nodes. In addition, an entry fee is received from nodes who want to participate in relaying messages in a community. The theoretical experiments prove that the efficiency loss of this scheme is $\frac{4}{8+M}$ where M is the number of network nodes. Chahin *et al.* [175] employ minority game to efficiently reward mobile nodes with respect to their mobility and resource consumption. The game aims to select a fraction of relay nodes (*i.e.,* the minority) that are willing to participate in relaying a message on behalf of a source node under imperfect state information. The objective is to achieve an optimal performance tradeoff between the delivery probability and resource consumptions.

A number of other game-theoretic incentive approaches are proposed in D2D communications. Huang *et al.* [176] propose a repeated game for inter-cell scenarios where a D2D link is located in the overlapping area of two neighboring cells. In particular, the BSs are considered as the game players that compete for the resource demands of D2D devices where their utility is using the radio resources for both cellular and D2D communications. Barua *et al.* [177] design a repeated game for cooperative content sharing in which a D2D node receives contents from the BS and broadcasts them to interested nodes. Since selfish nodes do not cooperate in data forwarding, the game takes the nodes' cooperation level into account to select the best content carriers. While nodes with high cooperation level are rewarded by the BS, selfish nodes are punished in the next round of the game by giving their interested contents through cellular links. Li *et al.* [178] design a mean filed game to encourage truth-telling about individual nodes states by paying monetary payments in a D2D real-time content streaming scenario. Furthermore, Zhang *et al.* [179] propose a signaling game-based incentive scheme for D2D content distribution wherein the main objective is to maximize the nodes' monetary profits while guaranteeing a non-negative utility for the BS.

Summary: Table V summarizes the incentive objectives, analytical tools, and the major performance results of our studied game-theoretic credit schemes. It can be seen that the Stackelberg game-based incentive mechanisms mainly model the interactions between a BS, cellular nodes, and D2D nodes where the main objective is to efficiently allocate the spectrum resources, minimize the cost of the BS while maximizing the utility of cellular and D2D nodes. The auction game-based methods primarily aim to maximize the system sum transmission rate where the nodes can obtain maximum resource units with minimum payments. While the existing Stackelberg and auction game-based incentive approaches focus on D2D communications, the bargaining game-based mechanisms model message trading between mobile nodes where Nash bargaining and subgame perfect equilibrium solutions are mainly employed to find the equilibrium points. In addition, the coalition formation game solutions model content distribution in multi-hop cluster-based D2D communication where the main objective is to stimulate nodes inside the coalitions to participate with each other in data distribution. Furthermore, the other game-based incentive approaches aim to stimulate D2D devices to collaborate in data sharing with each other while allocating the spectrum resources efficiently.

2) Security-Based Credit Mechanisms: Some existing studies incorporate security issues into credit mechanisms to protect them against various internal attacks (*e.g.,* edge insertion and edge removal) in which malicious nodes strive to maximize their reward but reduce the reward of honest nodes.

SMART [180] is a well-known secure pricing scheme in which the concept of *layered coin* is employed to secure the rewarding and achieve fairness. First, the source of a message generates the first layer of the coin to indicate the credit value and rewarding policy. Next, each intermediate node adds a new layer to the coin by attaching its digital signature to show its participation in relaying the message. Once the message is delivered, nodes in the delivery path share the credit according to a profit-sharing model. However, malicious nodes may insert or remove fake layers or collude with each other to gain extra rewards. To overcome these attacks, a layer concatenation technique is designed in which the information of the previous and next layers are attached to the current layer to protect the layered coins against such attacks. Similarly, Lu *et al.* [181] employ the concept of layered coin to secure the credit assignment in which the source nodes reward the nodes in the delivery path of successfully delivered messages. To achieve fairness, nodes participated in relay a message obtain a reputation even if the message is not successfully delivered to its destination. Chen *et al.* [182] introduce contribution time to reward relay nodes in the earliest delivery path of messages where the contribution time is the period of time between the receiving and forwarding of a message by a relay node. Using this method, a malicious node has no incentive to launch the edge insertion, removal, or content manipulate attacks because only nodes in the earliest delivery path receive credit.

Some security-based credit schemes aim at detecting layer insertion and removal attacks. Threshold incentive scheme [183] securely rewards the intermediate nodes for relaying a message where a time order-preserving aggregated

signature method is applied to detect the layer insertion attack. MuRIS [184] applies a rule to thwart the edge insertion attack in which the reward for relaying a message through an n-hop path must be equal or higher than the total rewards gained via an insertion attack.

3) Miscellaneous Credit Approaches: in addition to the game-theoretic and security-based mechanisms, some miscellaneous credit-based schemes have been proposed in the literature. Guan *et al.* [185] address the appearance of poverty nodes in DTNs in which SS nodes with strong social relations preferably choose each other as intermediate nodes to forward their messages, hence they gain more credit. Thus, it becomes difficult for nodes with fewer social relations to get sufficient rewards so that they can afford the cost of their forwarding messages. To deal with this problem, a taxation strategy is employed to fairly redistribute the credit among nodes and avoid the existence of poverty nodes. Mei and Stefa [186] propose Give2Get Epidemic and Give2Get Delegation protocols based on a cryptographic proof-based technique to stimulate SS nodes to relay messages received from their non-social nodes. CAIS [187] aims to stimulate IS and SS nodes to participate in message relaying by designing different charging and rewarding strategies for IS and SS nodes. In particular, social and non-social credit are rewarded to a node when it relays a message received from a node in the same community or other communities, respectively. Furthermore, a data replication controlling mechanism is designed, based on which the number of messages a node can replicate is limited based on its social and non-social credit.

Seregina *et al.* [188] design a reward-based incentive scheme for the Two-hop routing where the source of a message rewards only the first deliverer. Thus, intermediate nodes decide whether or not to relay a message based on the information provided by the source node. Specifically, three strategies are analyzed where the source can share information about the message in three settings: full (the number and ages of the message copies), partial (the number of the message copies), and no information. The experimental results reveal that the expected reward paid by a resource node is the same irrespective of the information provided to the relay node. Meanwhile, it is optimal for the source node to pretend that it is the first message replicator. DISCUSS [189] is an incentive-based data forwarding protocol based on evolutionary theory in which encountered nodes share their message forwarding history with each other that can help them to choose the best routing strategy dynamically. In DISCUSS, three types of nodes are considered: cooperators that relay messages for others altruistically; exploiters that use the capability of other nodes in data forwarding but do not relay their messages; and isolators that neither help nor get help. Thus, a node in DISCUSS selects the cooperators as the next message carriers as well as motives the exploiters and isolators to reveal their routing strategies and cooperate in message relaying.

Some recent incentive-based mobile data offloading mechanisms aim at encouraging mobile nodes to relay a portion of the cellular traffic through DTNs and Wi-Fi hotspots [29]. Zhou *et al.* [190] propose a reverse auction-based incentive approach, namely Win-Coupon, in which nodes with high

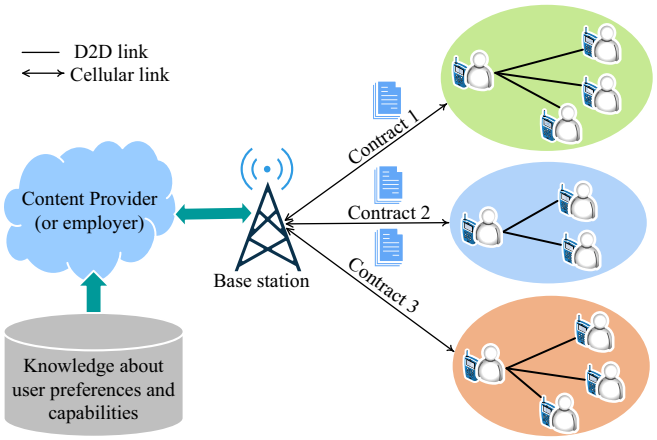

Fig. 9. A general illustration of contract-based incentive design.

delay tolerance and large offloading potentials have the highest priority to offload the cellular traffic. In Win-Coupon, auction-winning users receive data with delay and earn a coupon, whereas other nodes download data from the cellular network directly. In particular, a semi-Markov model is designed to predict the nodes' delay tolerance potentials based on their mobility patterns. Similarly, Li *et al.* [191] employ contract theory to model delayed data offloading between an operator and mobile nodes in which each mobile node chooses a proper contract based on its preferences. The main objective is to maximize the operator's profit while guaranteeing the feasibility of the nodes. Kouyoumdjieva and Karlsson [192] propose an energy-aware mobile data offloading algorithm, which combines duty cycling and selfishness energy saving mechanisms to promote the cooperation of mobile nodes. The experiments reveal that the proposed scheme achieves up to 85% energy savings while losing about 1% in system throughput when nodes fully cooperate in data distribution. In addition, it shows that the proposed scheme is robust against non-cooperative nodes even when 50% of the nodes do not follow the underlying data offloading protocol.

A number of miscellaneous incentive approaches have been proposed in D2D communication. Zhang *et al.* [31], [193] and Chen *et al.* [194] introduce the application of contract theory to model the interaction between content provider(s) and nodes where the main objective is to maximize the utility of the operator provided that the expected utility of nodes is also satisfied when signing the contract. In comparison to other incentive approaches (*e.g.,* auction games), contract-based methods can reduce nodes' computational and communication cost because the operator does not need to collect the nodes' feedback after each auction announcement. Instead, the operator provides different contracts and their corresponding rewards for nodes with different features, and the nodes can select a more beneficial contract with maximum benefits (Fig. 9).

Some incentive schemes for D2D communications group nodes into communities based on their social relationships or contact history and explore their incentives for inter and intra-group cooperations. Zhao *et al.* [50] propose a three-phase approach for data dissemination in which nodes are grouped

TABLE VI
SUMMARY OF THE SECURITY-BASED AND MISCELLANEOUS CREDIT MECHANISMS

Model	Reference	Principle of proposed solutions	Incentive objective	Specialties (+) and limitations (-)
Security-based credit approaches	Zhu *et al.* [180]	A multi-layer credit scheme based on layered coin	Dividing the total credit among the cooperative nodes based on a profit-sharing model	+ Detects the edge insertion and removal attacks
	Lu *et al.* [181]	A hybrid (credit and reputation) incentive that provides fairness	Maximizing the credit of nodes that deliver messages	+ Thwarts edge insertion and removal attacks - Considers the single-copy routing only
	Chen *et al.* [182]	An incentive-compatible scheme for the nodes that have a finite budget	Rewarding the nodes in the earliest delivery path based on the concept of contribution time	+ Detects the edge insertion, removal, and manipulation attacks - No evaluation of the communication cost
	Zhou and Cao [183]	A threshold incentive mechanism based on a modified population dynamic model	Rewarding the nodes for data relaying and security considerations	+ Considers fairness by providing equal relaying opportunities to each node - No evaluation of the communication cost
	Wang *et al.* [184]	A multi-receiver charging and rewarding scheme for data dissemination	Replicating messages to nodes that have already delivered previous messages successfully	+ Detects the edge insertion attacks - Cannot detect colluding attacks
Miscellaneous credit approaches	Guan *et al.* [185]	A taxation strategy to avoid the existence of poverty nodes caused by socially selfish behavior	Provides credit for socially isolated nodes to afford buy the forwarding services of other nodes	+ Introduces a new form of internal threats - Lack of analytical evaluations
	Mei and Stefa [186]	One of the first selfish-resilient social-aware data forwarding protocols	Pushing messages far from a local community swiftly with a minimum number of replications	+ The routing strategies are Nash equilibria Cannot detect colluding selfish nodes
	Ning *et al.* [187]	A community-based incentive scheme to stimulate both IS and SS nodes in data relaying	Maximizing the individual and the social utility of nodes	+ Applies different types of credit for nodes with different routing preferences - Lack of analytical evaluations
	Seregina *et al.* [188]	A credit scheme to promote the cooperation of nodes in Two-hop relaying	Minimizing the amount of prices to be paid for delivering messages	+ Every relay node is proposed a different reward based on its contact probability - Rewarding is unfair because only the first deliverer is rewarded
	Misra *et al.* [189]	A rewarding scheme in which nodes adapt their forwarding strategy based on message delivery information	Maximizing the delivery probability of messages by motivating selfish nodes to cooperation	+ Presenting both analytical and simulation-based experiments - No consideration of the nodes' social preferences
	Zhuo *et al.* [190]	An auction-based incentive mechanism that leverages nodes' delay tolerance for traffic offloading	Minimizing the incentive cost given an offloading target	+ Considers the dynamic features of nodes' delay tolerance - Nodes' social features are not considered
	Li *et al.* [191]	A contract-based incentive mechanism for data offloading with respect to nodes' satisfaction factors	Maximizing the operator's profit for both continuous and discrete user-type models	+ The operator can make decision based on nodes' statistical information - Node mobility is not considered
	Kouyoumdjieva and Karlsson [192]	An adaptable and scalable mobile data offloading protocol under full and limited node cooperation	Maximizing the network throughput while saving the nodes' energy	+ exploits the energy consumption of nodes that participate in the offloading process - Does not conduct analytical experiments
	Zhang *et al.* [193]	A contract-based mechanism to overcome the information asymmetry problem in D2D content sharing	Optimizing the network capacity while guaranteeing the network QoS requirements	+ A flexible rewarding method based on the nodes' preferences
	Chen *et al.* [194]	A general framework for designing optimal contracts between the operator and D2D nodes	Maximize the profit of service provider and nodes according to their valuations	+ The operator does not require gathering information from nodes frequently - Less communication and computational costs
	Zhao *et al.* [50]	A social and contact-based incentive scheme for community-based D2D data sharing	Maximizing the utility of nodes and their social friends with respect to their restricted resources	+ Selfish nodes are stimulated to truthfully report their data forwarding preferences
	Pan *et al.* [195]	A social-based incentive scheme for community-based D2D data offloading	Maximizing the data offloading gain considering the nodes' content and social preferences	+ Complimenting simulations with analytical results
	Wu *et al.* [56]	A social-aware rate-based D2D data sharing scheme, which is modeled as a maximum weighted mixed matching problem	Maximizing the individual utility of nodes	+ Considers a novel multi-hop D2D communication paradigm - Resource representations and scheduling techniques are not considered

into communities based on their betweenness centrality. Next, seed nodes in each community are identified according to their closeness centrality. Finally, they disseminate messages received from the BS to their socially-connected nodes in their community where the nodes in each community have an incentive to mutually benefit from exchanging messages with each other in a multi-hop D2D communication mode. Similarly, Pan *et al.* [195] propose a content pushing mechanism in which

nodes are grouped based on their content preferences where a node replicates contents for inter-group and intra-group nodes with different probabilities. The experiments demonstrate that the offloading performance heavily relies on the cooperation level of nodes. Wu *et al.* [56] propose a joint social-aware and link quality-based content sharing mode selection protocol in the presence of cooperative and SS nodes. It is assumed that there exist three communication models: BS-to-D2D, D2D, and multi-hop D2D. Thus, the content sharing mode selection problem is modeled as a maximum mixed matching problem.

Summary: Table VI summarizes the main characteristics of the security-based and miscellaneous credit mechanisms. It can be seen that the majority of the security-based rewarding schemes use the layered coin technique to protect granting rewards to cooperative nodes and protect the rewarding system against malicious attacks. In addition, almost all the security-based credit schemes focus on DTNs, while the security of credit distribution in D2D communications is not studied in the existing works. Furthermore, the miscellaneous credit mechanisms employ concepts, such as taxation, contract theory, and social community to design their incentive mechanisms.

VI. Open Discussion and Future Directions

In previous sections, we have reviewed the state-of-the-art of data routing and dissemination services and protocols in the non-cooperative WRNs and highlighted their specialties and limitations. In light of the works focusing on various aspects of the non-cooperative WRNs, there are still several open problems and challenges, which are left without proper answers. In this section, we discuss possible future research directions that can bring new visions into the horizon of WRNs.

A. Realistic Human Altruism and Selfishness Models

So far, we introduced different types of human selfish behaviors and actions in WRNs (*e.g.,* [59] and [83]). Although IS and SS nodes have been introduced as general selfishness models, several other important factors (such as available resources, content knowledge, and spatiotemporal information) should be further explored to realistically model the selfish behavior of mobile nodes in WRNs. For example, it is challenging how the selfish behavior of mobile nodes evolves in different situations and locations based on their social and contextual properties. In addition, it is non-trivial to explore how the selfish behavior of nodes changes when different levels of battery or power resources remain in their devices (or when their devices are charging). Modeling human selfish behaviors in D2D communication with respect to its unique characteristics is another challenging issue that received less attention from the research community. For example, it is not explored how much selfish D2D nodes have the freedom to limit sharing their spectrum resources with other nodes. Moreover, how their social tie information and relationships affect their cooperation levels in content sharing and distribution.

B. Impact Analysis of Human Non-Cooperative Behaviors on Data Forwarding and Content Sharing

Although the impact of mobile nodes' non-cooperative behaviors on the performance of data delivery protocols in DTNs has been studied from different perspectives (see Section III), several avenues for further research are still open. The existing analytical models have generally explored the effects of nodes' selfish behavior on only the data delivery delay and transmission cost metrics (see Table I). One future trend is extending the existing analytical frameworks to a generic model (*e.g.,* a multi-dimensional CTMC model) to analyze the performance depredation of other system parameters (such as the data delivery ratio and energy) and compare their tradeoffs. In addition, exploring the impact of nodes' sophisticated selfish behavior on the overall performance of data delivery raises new research problems. For example, it is non-trivial to explore how nodes' social ties, physical locations, or contextual information affect their cooperation level and the performance of data delivery protocols under different settings (*e.g.,* when the network traffic varies from medium to high).

The impact of mobile nodes' selfish behavior on the overall D2D network performance is another interesting research challenge that received less attention by the research community. Although a limited number of simulation-based experiments (*e.g.,* [86] and [88]) have studied human selfish behaviors in D2D communications underlying cellular networks, there is no analytical approach to explore the effects' of node selfishness on network throughput accurately. For example, a CTMC model can be designed to model data dissemination in community-based D2D communications and analyze how the network performance metrics are degraded in the presence of D2D selfish mobile nodes. Additionally, specific communication protocols and policies (*e.g.,* opportunistic scheduling algorithms) should be developed to determine human cooperation models and control the system parameters against changes made by D2D selfish mobile nodes.

C. Robust Mechanisms to Detect Non-Cooperative Nodes

Although different mechanisms are proposed to detect selfish and malicious mobile nodes in WRNs (see Section IV), they might be ineffective and inefficient in case the number of malicious nodes is high or sophisticated denial-of-service attacks are launched by them. The main reason is that mobile nodes often do not have up-to-date information about the network's global state (*i.e.,* the contact and social graphs), especially in highly dynamic WRNs. One promising solution to effectively detect non-cooperative nodes is establishing trust relationships among nodes based on their social similarities or analyzing their data forwarding behaviors based on their social preferences (see [196]). This idea sounds very useful because the social features of nodes are relatively stable over time. Another possible solution is developing a learning system based on nodes' contact history or social relations to discover the patterns of common selfishness and attack models. In such a system, mobile nodes can upload their contact

and social properties to a server and the server runs complicated operations to learn the nodes' behavior and find their selfishness and attack patterns. Detecting colluding attackers in WRNs is another challenging problem, which is addressed by a few numbers of recent studies (*e.g.,* in [116]). While the majority of the existing detection methods investigate nodes' contact history to discover inconsistent or manipulated records, exploring the contact graph (instead of contact history) can help detect colluding attackers swiftly and accurately.

Establishing secure and reliable data sharing and dissemination protocols in D2D communications by selecting honest and trustworthy intermediate nodes and isolating selfish and malicious nodes is a greatly challenging problem. For example, it is non-trivial to explore how to detect D2D selfish nodes in heterogeneous and large-scale networks when they use unlicensed bands to share their messages. One promising solution could be to design distributed and decentralized security and trustworthy mechanisms in which novel technologies (such as blockchain) are employed to store and exchange nodes' security information and control their cooperation and trustworthiness. Another exciting research direction is to detect malicious nodes and their attack models in D2D communications, which is not explored in the literature.

D. Effective and Fair Incentive Mechanisms

Different incentive mechanisms have been proposed to stimulate the cooperation of selfish nodes in WRNs (see Section V). Overall, it can be seen that effectiveness and fairness are two important factors that should be considered in designing an incentive mechanism. In other words, an incentive scheme should not only appropriately encourage selfish nodes to help relay messages on behalf of other nodes but also reward the nodes according to their cooperation level fairly and protect the rewarding system against malicious attacks and unfair manipulations. One major challenge in providing effective incentives is to devise various forms of incentives (*e.g.,* monetary, social relevance, or non-monetary) to stimulate the cooperation of nodes with different selfish behaviors and preferences. For example, empirical experiments in [83] reveal that minor credit (*e.g.,* one dollar) can change the altruistic behavior of mobile users with limited device resources significantly. In addition, taking into account the properties of contents (*e.g.,* their size) and the actual capabilities of nodes for data distribution (*e.g.,* the energy level of their devices) can help design effective incentive mechanisms.

Another challenging future research direction is developing effective incentive strategies in D2D-enabled heterogeneous networks that can ultimately raise cooperation among wireless D2D nodes, spectrum owners, and service providers. Due to the bandwidth limitations of the backhaul network and base stations in the heterogeneous networks, encouraging resource-limited D2D devices to cache contents for others and share their spectrum resources with them is extremely challenging, especially for data-intensive applications with massive users. To effectively stimulate D2D devices to cooperate with the other network entities in data delivery, different criteria, such as resource availability and user interests in content should be considered. For example, different cost and rewarding mechanisms can be considered for users with different preferences. One promising solution is applying cooperative and non-cooperative game-theoretic approaches to analyze multi-stage interactions between the base station and D2D devices with heterogeneous resources, reveal their true preferences, and maximize their utilities.

Developing secure and privacy-preserving incentive mechanisms in the presence of malicious and cheating nodes are other important research challenges that need further explorations. For instance, how to design secure incentive mechanisms that enforce the required fairness in assigning rewards to cooperative nodes is still an open problem. Besides, it remains an important issue how to stimulate mobile nodes to cooperate in data delivery, consume their computational, and bandwidth resources while preserving their privacy.

VII. Conclusion

In this paper, we presented an in-depth literature review of recent studies on human-centric communications in non-cooperative WRNs. Specifically, we introduced different selfish behavior and malicious attacks that can be launched by misbehaving nodes in cooperative data delivery. Meanwhile, we studied the impacts of nodes' different non-cooperative actions on the performance of data delivery protocols. In addition, we discussed distributed detect and defense mechanisms that attempt to identify selfish and malicious nodes in WRNs. Furthermore, we explored a large number of incentive mechanisms and discussed their major characteristics. Finally, we discussed several open issues and future research directions. Since efficient and secure communications are simultaneously becoming ever-important in next-generation wireless networks, we hope that this survey will be useful for the network protocol and mobile application developers and encourage them to design appealing data delivery mechanisms.

Acknowledgment

The authors are grateful to the anonymous reviewers for their constructive comments and suggestions to improve the quality of the article.

References

[1] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021*, Cisco, San Jose, CA, USA, 2016. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

[2] K. Fall, "A delay-tolerant network architecture for challenged Internets," in *Proc. ACM SIGCOMM*, Karlsruhe, Germany, 2003, pp. 27–34.

[3] T. S. Athanasios V. Vasilakos, and Y. Zhang, *Delay Tolerant Networks: Protocols and Applications*. Boca Raton, FL, USA: CRC Press, 2011.

[4] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014.

[5] X. Hu *et al.*, "A survey on mobile social networks: Applications, platforms, system architectures, and future research directions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1557–1581, 3rd Quart., 2015.

[6] V. Sciancalepore, D. Giustiniano, A. Banchs, and A. Hossmann-Picu, "Offloading cellular traffic through opportunistic communications: Analysis and optimization," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 1, pp. 122–137, Jan. 2016.

[7] K. W. Choi and Z. Han, "Device-to-device discovery for proximity-based service in LTE-advanced system," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 55–66, Jan. 2015.

[8] S.-Y. Lien *et al.*, "Enhanced LTE device-to-device proximity services," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 174–182, Dec. 2016.

[9] Y. Zeng, K. Xiang, D. Li, and A. V. Vasilakos, "Directional routing and scheduling for green vehicular delay tolerant networks," *Wireless Netw.*, vol. 19, no. 2, pp. 161–173, 2013.

[10] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 16–55, May 2017.

[11] N. Kayastha, D. Niyato, P. Wang, and E. Hossain, "Applications, architectures, and protocol design issues for mobile social networks: A survey," *Proc. IEEE*, vol. 99, no. 12, pp. 2130–2158, Dec. 2011.

[12] Z. Mao *et al.*, "Mobile social networks: Design requirements, architecture, and state-of-the-art technology," *Comput. Commun.*, vol. 100, pp. 1–19, Mar. 2017.

[13] N. Vastardis and K. Yang, "Mobile social networks: Architectures, social properties, and key research challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1355–1371, 3rd Quart., 2013.

[14] Y. Wang, A. V. Vasilakos, Q. Jin, and J. Ma, "Survey on mobile social networking in proximity (MSNP): Approaches, challenges and architecture," *Wireless Netw.*, vol. 20, no. 6, pp. 1295–1311, 2014.

[15] K. Wei, X. Liang, and K. Xu, "A survey of social-aware routing protocols in delay tolerant networks: Applications, taxonomy and design-related issues," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 556–578, 1st Quart., 2014.

[16] K. Zhu, W. Li, X. Fu, and L. Zhang, "Data routing strategies in opportunistic mobile social networks: Taxonomy and open challenges," *Comput. Netw.*, vol. 93, no. 1, pp. 183–198, Dec. 2015.

[17] N. Chakchouk, "A survey on opportunistic routing in wireless communication networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2214–2241, 4th Quart., 2015.

[18] T. Spyropoulos, R. N. B. Rais, T. Turletti, K. Obraczka, and A. Vasilakos, "Routing for disruption tolerant networks: Taxonomy and design," *Wireless Netw.*, vol. 16, no. 8, pp. 2349–2370, 2010.

[19] I. Woungang, S. K. Dhurandher, A. Anpalagan, and A. V. Vasilakos, *Routing in Opportunistic Networks*. New York, NY, USA: Springer, 2013.

[20] M. Youssef, M. Ibrahim, M. Abdelatif, L. Chen, and A. V. Vasilakos, "Routing metrics of cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 92–109, 1st Quart., 2014.

[21] T. Abdelkader, K. Naik, A. Nayak, N. Goel, and V. Srivastava, "A performance comparison of delay-tolerant network routing protocols," *IEEE Netw.*, vol. 30, no. 2, pp. 46–53, Mar./Apr. 2016.

[22] Y. Zhu, B. Xu, X. Shi, and Y. Wang, "A survey of social-based routing in delay tolerant networks: Positive and negative social effects," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 387–401, 1st Quart., 2013.

[23] S. Batabyal and P. Bhaumik, "Mobility models, traces and impact of mobility on opportunistic routing algorithms: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1679–1707, 3rd Quart., 2015.

[24] P. Pirozmand, G. Wu, B. Jedari, and F. Xia, "Human mobility in opportunistic networks: Characteristics, models and prediction methods," *J. Netw. Comput. Appl.*, vol. 42, pp. 45–58, Jun. 2014.

[25] L. Jin, Y. Chen, T. Wang, P. Hui, and A. V. Vasilakos, "Understanding user behavior in online social networks: A survey," *IEEE Commun. Mag.*, vol. 51, no. 9, pp. 144–150, Sep. 2013.

[26] Y.-Q. Zhang, X. Li, J. Xu, and A. V. Vasilakos, "Human interactive patterns in temporal networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 2, pp. 214–222, Feb. 2015.

[27] Y. Li, M. Qian, D. Jin, P. Hui, and A. V. Vasilakos, "Revealing the efficiency of information diffusion in online social networks of microblog," *Inf. Sci.*, vol. 293, pp. 383–389, Feb. 2015.

[28] B. M. C. Silva, J. J. P. C. Rodrigues, N. Kumar, and G. Han, "Cooperative strategies for challenged networks and applications: A survey," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2749–2760, Dec. 2017.

[29] Y. He, M. Chen, B. Ge, and M. Guizani, "On WiFi offloading in heterogeneous networks: Various incentives and trade-off strategies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2345–2385, 4th Quart., 2016.

[30] G. Iosifidis, L. Gao, J. Huang, and L. Tassiulas, "Social-oriented adaptive transmission in opportunistic Internet of smartphones," *IEEE Commun. Mag.*, vol. 52, no. 9, pp. 20–27, Dec. 2014.

[31] Y. Zhang, M. Pan, L. Song, Z. Dawy, and Z. Han, "A survey of contract theory-based incentive mechanism design in wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 80–85, Jun. 2017.

[32] A. M. Ahmed, T. Qiu, F. Xia, B. Jedari, and S. Abolfazli, "Event-based mobile social networks: Services, technologies, and applications," *IEEE Access*, vol. 2, pp. 500–513, 2014.

[33] Y. Wang, L. Wei, A. V. Vasilakos, and Q. Jin, "Device-to-device based mobile social networking in proximity (MSNP) on smartphones: Framework, challenges and prototype," *Future Gener. Comput. Syst.*, vol. 74, pp. 241–253, Sep. 2017.

[34] Y. Zhao and W. Song, "Survey on social-aware data dissemination over mobile wireless networks," *IEEE Access*, vol. 5, pp. 6049–6059, 2017.

[35] P. Gandotra, R. K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," *J. Netw. Comput. Appl.*, vol. 78, pp. 9–29, Jan. 2017.

[36] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Social-aware resource allocation and optimization for D2D communication," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 122–129, Jun. 2017.

[37] Y. Najaflou, B. Jedari, F. Xia, L. T. Yang, and M. S. Obaidat, "Safety challenges and solutions in mobile social networks," *IEEE Syst. J.*, vol. 9, no. 3, pp. 834–854, Sep. 2015.

[38] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and privacy in mobile social networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 21, no. 1, pp. 33–41, Feb. 2014.

[39] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[40] M. Haus *et al.*, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.

[41] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *Proc. 33rd Annu. Conf. IEEE Ind. Electron. Soc.*, Taipei, Taiwan, 2007, pp. 46–51.

[42] F. Xia, L. Liu, J. Li, J. Ma, and A. V. Vasilakos, "Socially aware networking: A survey," *IEEE Syst. J.*, vol. 9, no. 3, pp. 904–921, Sep. 2015.

[43] F. Xia, A. M. Ahmed, L. T. Yang, J. Ma, and J. J. P. C. Rodrigues, "Exploiting social relationship to enable efficient replica allocation in ad-hoc social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3167–3176, Dec. 2014.

[44] F. Xia *et al.*, "BEEINFO: Interest-based forwarding using artificial bee colony for socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 64, no. 3, pp. 1188–1200, Mar. 2015.

[45] J. Li *et al.*, "Geo-social distance-based data dissemination for socially aware networking," *IEEE Access*, vol. 4, pp. 1444–1453, 2016.

[46] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic Internet of smartphones," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 810–820, Apr. 2017.

[47] Y. Meng, C. Jiang, H.-H. Chen, and Y. Ren, "Cooperative device-to-device communications: Social networking perspectives," *IEEE Netw.*, vol. 31, no. 3, pp. 38–44, May/Jun. 2017.

[48] Y. Li, T. Wu, P. Hui, D. Jin, and S. Chen, "Social-aware D2D communications: Qualitative insights and quantitative analysis," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 150–158, Jun. 2014.

[49] Y. Zhang *et al.*, "Social network aware device-to-device communication in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 177–190, Jan. 2015.

[50] Y. Zhao, W. Song, and Z. Han, "Social-aware data dissemination via device-to-device communications: Fusing social and mobile networks with incentive constraints," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2016.2599160.

[51] B. Zhang, Y. Li, D. Jin, P. Hui, and Z. Han, "Social-aware peer discovery for D2D communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2426–2439, May 2015.

[52] Y. Zhao, Y. Li, Y. Cao, T. Jiang, and N. Ge, "Social-aware resource allocation for device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6621–6634, Dec. 2015.

[53] L. Militano *et al.*, "Trust-based and social-aware coalition formation game for multihop data uploading in 5G systems," *Comput. Netw.*, vol. 111, pp. 141–151, Dec. 2016.

[54] A. Ometov *et al.*, "A novel security-centric framework for D2D connectivity based on spatial and social proximity," *Comput. Netw.*, vol. 107, pp. 327–338, Oct. 2016.

[55] R. Wang, K. Liu, D. Wu, H. Wang, and J. Yan, "Malicious-behavior-aware D2D link selection mechanism," *IEEE Access*, vol. 5, pp. 15162–15173, 2017.

[56] D. Wu, L. Zhou, and Y. Cai, "Social-aware rate based content sharing mode selection for D2D content sharing scenarios," *IEEE Trans. Multimedia*, vol. 19, no. 11, pp. 2571–2582, Nov. 2017.

[57] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, 2017.

[58] Y. Cao, T. Jiang, and C. Wang, "Cooperative device-to-device communications in cellular networks," *IEEE Wireless Commun.*, vol. 22, no. 3, pp. 124–129, Jun. 2015.

[59] P. Hui *et al.*, "Selfishness, altruism and message spreading in mobile social networks," in *Proc. IEEE INFOCOM Workshops*, Rio de Janeiro, Brazil, 2009, pp. 1–6.

[60] A. Keranen, M. Pitkänen, M. Vuori, and J. Ott, "Effect of non-cooperative nodes in mobile DTNs," in *Proc. IEEE WoWMoM*, Lucca, Italy, 2011, pp. 1–7.

[61] A. Panagakis, A. Vaios, and L. Stavrakakis, "On the effects of cooperation in DTNs," in *Proc. 2nd Int. Conf. Commun. Syst. Softw. Middleware*, Bengaluru, India, 2007, pp. 1–6.

[62] S. T. Kouyoumdjieva and G. Karlsson, "The virtue of selfishness: Device perspective on mobile data offloading," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, New Orleans, LA, USA, 2015, pp. 2067–2072.

[63] V. K. C. Manam, V. Mahendran, and C. S. R. Murthy, "Performance modeling of DTN routing with heterogeneous and selfish nodes," *Wireless Netw.*, vol. 20, no. 1, pp. 25–40, 2014.

[64] Q. Li, W. Gao, S. Zhu, and G. Cao, "A routing protocol for socially selfish delay tolerant networks," *Ad Hoc Netw.*, vol. 10, no. 8, pp. 1619–1632, 2012.

[65] E. Jaho, M. Karaliopoulos, and I. Stavrakakis, "Social similarity favors cooperation: The distributed content replication case," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 601–613, Mar. 2013.

[66] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[67] A. Ometov *et al.*, "Toward trusted, social-aware D2D connectivity: Bridging across the technology and sociality realms," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 103–111, Aug. 2016.

[68] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 594–605, Jan. 2016.

[69] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social Internet of Things systems," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov./Dec. 2016.

[70] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Dept. Comput. Sci., Duke Univ., Durham, NC, USA, Rep. CS-200006, 2000.

[71] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 4, pp. 477–486, Aug. 2002.

[72] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," in *Proc. ACM SIGCOMM*, Philadelphia, PA, USA, 2005, pp. 252–259.

[73] A. Dvir and A. V. Vasilakos, "Backpressure-based routing protocol for DTNs," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 405–406, 2010.

[74] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE Comput. Commun. Rev.*, vol. 7, no. 3, pp. 19–20, 2003.

[75] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE Rap: Social-based forwarding in delay-tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 11, pp. 1576–1589, Nov. 2011.

[76] W. Moreira, P. Mendes, and S. Sargento, "Opportunistic routing based on daily routines," in *Proc. IEEE WoWMoM*, San Francisco, CA, USA, 2012, pp. 1–6.

[77] F. Xia, L. Liu, B. Jedari, and S. K. Das, "PIS: A multi-dimensional routing protocol for socially-aware networking," *IEEE Trans. Mobile Comput.*, vol. 15, no. 11, pp. 2825–2836, Nov. 2016.

[78] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks," *IEEE Commun. Lett.*, vol. 14, no. 11, pp. 1026–1028, Nov. 2010.

[79] M. Karaliopoulos, "Assessing the vulnerability of DTN data relaying schemes to node selfishness," *IEEE Commun. Lett.*, vol. 13, no. 12, pp. 923–925, Dec. 2009.

[80] Y. Li, G. Su, and Z. Wang, "Evaluating the effects of node cooperation on DTN routing," *AEU Int. J. Electron. Commun.*, vol. 66, no. 1, pp. 62–67, 2012.

[81] G. Resta and P. Santi, "A framework for routing performance analysis in delay tolerant networks with application to noncooperative networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 1, pp. 2–10, Jan. 2012.

[82] X. Xiao, Y. Li, X. Kui, and A. V. Vasilakos, "Assessing the influence of selfishness on the system performance of gossip based vehicular networks," *Wireless Netw.*, vol. 20, no. 7, pp. 1795–1805, 2014.

[83] C. Bermejo, R. Zheng, and P. Hui, "An empirical study of human altruistic behaviors in opportunistic networks," in *Proc. 7th Int. Workshop Hot Topics Planet Scale mObile Comput. Online Soc. neTw.*, Hangzhou, China, 2015, pp. 43–48.

[84] F. Xia, B. Jedari, L. T. Yang, J. Ma, and R. Huang, "A signaling game for uncertain data delivery in selfish mobile social networks," *IEEE Trans. Comput. Soc. Syst.*, vol. 3, no. 2, pp. 100–112, Jun. 2016.

[85] Y. Wang, A. V. Vasilakos, J. Ma, and N. Xiong, "On studying the impact of uncertainty on behavior diffusion in social networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 2, pp. 185–197, Feb. 2015.

[86] T. Wang, Y. Sun, L. Song, and Z. Han, "Social data offloading in D2D-enhanced cellular networks by network formation games," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 7004–7015, Dec. 2015.

[87] F. Wang, Z. Wang, and Z. Yang, "Evaluating the influence of social selfishness on cooperative D2D communications," in *Proc. 7th Int. Workshop Hot Topics Planet Scale mObile Comput. Online Soc. neTw. (HOTPOST)*, Hangzhou, China, 2015, pp. 49–54.

[88] C. Gao *et al.*, "Impact of selfishness in device-to-device communication underlying cellular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9338–9349, Oct. 2017.

[89] Y. Li *et al.*, "The impact of node selfishness on multicasting in delay tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 5, pp. 2224–2238, Jun. 2011.

[90] Y. Wu, S. Deng, and H. Huang, "On modeling the impact of selfish behaviors on limited epidemic routing in delay tolerant networks," *Wireless Pers. Commun.*, vol. 71, no. 4, pp. 2759–2782, 2013.

[91] P. Sermpezis and T. Spyropoulos, "Understanding the effects of social selfishness on the performance of heterogeneous opportunistic networks," *Comput. Commun.*, vol. 48, pp. 71–83, Jul. 2014.

[92] P. Sermpezis and T. Spyropoulos, "Delay analysis of epidemic schemes in sparse and dense heterogeneous contact networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 9, pp. 2464–2477, Sep. 2017.

[93] A. Asadi and V. Mancuso, "A survey on opportunistic scheduling in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1671–1688, 4th Quart., 2013.

[94] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[95] M. N. Mejri and J. Ben-Othman, "Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks," in *Proc. IEEE Glob. Commun. Conf.*, Austin, TX, USA, 2014, pp. 5032–5037.

[96] E. Hernández-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Evaluation of collaborative selfish node detection in MANETs and DTNs," in *Proc. 15th ACM Int. Conf. Model. Anal. Simulat. Wireless Mobile Syst. (MSWiM)*, Paphos, Cyprus, 2012, pp. 159–166.

[97] E. Hernández-Orallo, M. D. S. Olmos, J. C. Cano, C. T. Calafate, and P. Manzoni, "CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1162–1175, Jun. 2015.

[98] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 9, pp. 1514–1531, Sep. 2012.

[99] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7929–7937, Dec. 2015.

[100] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 22–32, Jan. 2014.

[101] S. Trifunovic, F. Legendre, and C. Anastasiades, "Social trust in opportunistic networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–6.

假设太多，未必有用

[102] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.

[103] G. Bigwood and T. Henderson, "IRONMAN: Using social networks to add incentives and reputation to opportunistic networks," in *Proc. IEEE 3rd Int. Conf. Soc. Comput.*, Boston, MA, USA, 2011, pp. 65–72.

[104] R.-I. Ciobanu, C. Dobre, M. Dascălu, S. Trăuşan-Matu, and V. Cristea, "SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks," *J. Netw. Comput. Appl.*, vol. 41, pp. 240–249, May 2014.

[105] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 5, pp. 1200–1210, May 2014.

[106] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Exploiting social ties for cooperative D2D communications: A mobile social networking case," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1471–1484, Oct. 2015.

[107] L. Militano *et al.*, "Trusted D2D-based data uploading in in-band narrowband-IoT with social awareness," in *Proc. IEEE 27th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Valencia, Spain, 2016, pp. 1–6.

[108] M. Zhang, X. Chen, and J. Zhang, "Social-aware relay selection for cooperative networking: An optimal stopping approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, 2014, pp. 2257–2262.

有趣 可以作为参考文献

[109] J. Yan, D. Wu, S. Sanyal, and R. Wang, "Trust-oriented partner selection in D2D cooperative communications," *IEEE Access*, vol. 5, pp. 3444–3453, 2017.

[110] Y. Cao, T. Jiang, X. Chen, and J. Zhang, "Social-aware video multicast based on device-to-device communications," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1528–1539, Jun. 2016.

[111] J. von Mulert, I. Welch, and W. K. G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV," *J. Netw. Comput. Appl.*, vol. 35, no. 4, pp. 1249–1259, 2012.

[112] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009, pp. 2428–2436.

[113] G. Dini and A. L. Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1167–1178, 2012.

[114] Q. Li and G. Cao, "Mitigating routing misbehavior in disruption tolerant networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 664–675, Apr. 2012.

[115] M. Alajeely, R. Doss, A. Ahmad, and V. Mak-Hau, "Catabolism attack and anabolism defense: A novel attack and traceback mechanism in opportunistic networks," *Comput. Commun.*, vol. 71, pp. 111–118, Nov. 2015.

[116] T. N. D. Pham and C. K. Yeo, "Detecting colluding blackhole and greyhole attacks in delay tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 5, pp. 1116–1129, May 2016.

[117] S. Saha *et al.*, "Design of efficient lightweight strategies to combat DoS attack in delay tolerant network routing," *Wireless Netw.*, vol. 24, no. 1, pp. 173–194, 2018.

[118] H. Kim, R. B. Chitti, and J. Song, "Novel defense mechanism against data flooding attacks in wireless ad hoc networks," *IEEE Trans. Consum. Electron.*, vol. 56, no. 2, pp. 579–582, May 2010.

[119] B. Liu *et al.*, "SF-DRDoS: The store-and-flood distributed reflective denial of service attack," *Comput. Commun.*, vol. 69, pp. 107–115, Sep. 2015.

[120] Q. Li, W. Gao, S. Zhu, and G. Cao, "To lie or to comply: Defending against flood attacks in disruption tolerant networks," *IEEE Trans. Depend. Secure Comput.*, vol. 10, no. 3, pp. 168–182, May/Jun. 2013.

[121] P. T. N. Diep and C. K. Yeo, "Detecting flooding attack while accommodating burst traffic in delay tolerant networks," in *Proc. Wireless Telecommun. Symp. (WTS)*, Chicago, IL, USA, 2017, pp. 1–7.

[122] I. Parris and T. Henderson, "Friend or flood? Social prevention of flooding attacks in mobile opportunistic networks," in *Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Madrid, Spain, 2014, pp. 16–21.

[123] F. Nait-Abdesselam, B. Bensaou, and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 127–133, Apr. 2008.

[124] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting wormhole attacks in delay-tolerant networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 36–42, Oct. 2010.

[125] T. N. D. Pham and C. K. Yeo, "Statistical wormhole detection and localization in delay tolerant networks," in *Proc. IEEE 11th Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2014, pp. 380–385.

[126] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A near-optimal social network defense against Sybil attacks," *IEEE/ACM Trans. Netw.*, vol. 18, no. 3, pp. 885–898, Jun. 2010.

[127] X. Lin, "LSR: Mitigating zero-day Sybil vulnerability in privacy-preserving vehicular peer-to-peer networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 237–246, Sep. 2013.

[128] S. Trifunovic and A. Hossmann-Picu, "Stalk and lie—The cost of Sybil attacks in opportunistic networks," *Comput. Commun.*, vol. 73, pp. 66–79, Jan. 2016.

[129] X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 310–320, Feb. 2014.

[130] Y. Sun, L. Yin, and W. Liu, "Defending Sybil attacks in mobile social networks," in *Proc. IEEE INFOCOM WKSHPS*, Toronto, ON, Canada, 2014, pp. 163–164.

[131] D. Quercia and S. Hailes, "Sybil attacks against mobile users: Friends and foes to the rescue," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–5.

[132] W. Chang, J. Wu, C. C. Tan, and F. Li, "Sybil defenses in mobile social networks," in *Proc. IEEE GLOBECOM*, Atlanta, GA, USA, 2013, pp. 641–646.

[133] K. Zhang, X. Liang, R. Lu, K. Yang, and X. S. Shen, "Exploiting mobile social behaviors for Sybil detection," in *Proc. IEEE INFOCOM*, Hong Kong, 2015, pp. 271–279.

[134] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in DTNs," in *Proc. IEEE Int. Conf. Netw. Protocols*, Orlando, FL, USA, 2008, pp. 238–247.

[135] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," *Ad Hoc Netw.*, vol. 8, no. 1, pp. 1–14, 2010.

[136] A. Krifa, C. Barakat, and T. Spyropoulos, "MobiTrade: Trading content in disruption tolerant networks," in *Proc. 6th ACM Workshop Challenged Netw. (CHANTS)*, Las Vegas, NV, USA, 2011, pp. 31–36.

[137] H. Zhou, J. Chen, J. Fan, Y. Du, and S. Das, "ConSub: Incentive-based content subscribing in selfish opportunistic mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 669–679, Sep. 2013.

[138] Y.-P. Hsu and L. Duan, "To motivate social grouping in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 4880–4893, Aug. 2017.

[139] L. Pu, X. Chen, J. Xu, and X. Fu, "D2D fogging: An energy-efficient and incentive-aware task offloading framework via network-assisted D2D collaboration," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3887–3901, Dec. 2016.

[140] N. Mastronarde, V. Patel, J. Xu, L. Liu, and M. van der Schaar, "To relay or not to relay: Learning device-to-device relaying strategies in cellular networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1569–1585, Jun. 2016.

[141] L. Wei, Z. Cao, and H. Zhu, "MobiGame: A user-centric reputation based incentive protocol for delay/disruption tolerant networks," in *Proc. IEEE GLOBECOM*, Kathmandu, Nepal, 2011, pp. 1–5.

[142] B. M. C. Silva, J. J. P. C. Rodrigues, N. Kumar, M. L. Proença, Jr., and G. Han, "MobiCoop: An incentive-based cooperation solution for mobile applications," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 12, no. 4, pp. 1–23, Aug. 2016.

[143] M. Salehi and A. Boukerche, "A comprehensive reputation system to improve the security of opportunistic routing protocols in wireless networks," in *Proc. IEEE GLOBECOM*, San Diego, CA, USA, 2015, pp. 1–6.

[144] D. Yang, X. Fang, and G. Xue, "Game theory in cooperative communications," *IEEE Wireless Commun.*, vol. 19, no. 2, pp. 44–49, Apr. 2012.

[145] L. Song, D. Niyato, Z. Han, and E. Hossain, "Game-theoretic resource allocation methods for device-to-device communication," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 136–144, Jun. 2014.

[146] F. Wang, L. Song, Z. Han, Q. Zhao, and X. Wang, "Joint scheduling and resource allocation for device-to-device underlay communication," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Shanghai, China, 2013, pp. 134–139.

[147] K. Sugiyama, T. Kubo, A. Tagami, and A. Parekh, "Incentive mechanism for DTN-based message delivery services," in *Proc. IEEE GLOBECOM*, Atlanta, GA, USA, 2013, pp. 3108–3113.

[148] Z. Chen, Y. Liu, B. Zhou, and M. Tao, "Caching incentive design in wireless D2D networks: A Stackelberg game approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, 2016, pp. 1–6.

[149] R. Yin *et al.*, "Joint spectrum and power allocation for D2D communications underlaying cellular networks," *IEEE Trans.Veh. Technol.*, vol. 65, no. 4, pp. 2182–2195, Apr. 2016.

[150] H. Wu and H. Ma, "Quality-oriented incentive mechanism for video delivery in opportunistic networks," in *Proc. IEEE Int. Symp. World Wireless Mobile Multimedia Netw.*, Sydney, NSW, Australia, 2014, pp. 1–6.

[151] Q. Wang, W. Wang, S. Jin, H. Zhu, and N. T. Zhang, "Quality-optimized joint source selection and power control for wireless multimedia D2D communication using Stackelberg game," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3755–3769, Aug. 2015.

[152] D. Wu, J. Yan, H. Wang, D. Wu, and R. Wang, "Social attribute aware incentive mechanism for device-to-device video distribution," *IEEE Trans. Multimedia*, vol. 19, no. 8, pp. 1908–1920, Aug. 2017.

[153] C. Xu *et al.*, "Interference-aware resource allocation for device-to-device communications as an underlay using sequential second price auction," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, 2012, pp. 445–449.

[154] C. Xu *et al.*, "Efficiency resource allocation for device-to-device underlay communication systems: A reverse iterative combinatorial auction based approach," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 348–358, Sep. 2013.

[155] S. Huang, C. Yi, and J. Cai, "A sequential posted price mechanism for D2D content sharing communications," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–6.

[156] M. H. Hajiesmaili, L. Deng, M. Chen, and Z. Li, "Incentivizing device-to-device load balancing for cellular networks: An online auction design," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 2, pp. 265–279, Feb. 2017.

[157] T. Ning, Z. Yang, X. Xie, and H. Wu, "Incentive-aware data dissemination in delay-tolerant mobile networks," in *Proc. 8th Annu. IEEE Commun. Soc. Conf. Sensor Mesh Ad Hoc Commun. Netw.*, Salt Lake City, UT, USA, 2011, pp. 539–547.

[158] T. Ning, Z. Yang, H. Wu, and Z. Han, "Self-interest-driven incentives for ad dissemination in autonomous mobile social networks," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2310–2318.

[159] F. Wu, T. Chen, S. Zhong, C. Qiao, and G. Chen, "A game-theoretic approach to stimulate cooperation for probabilistic routing in opportunistic networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 4, pp. 1573–1583, Apr. 2013.

[160] Y. Li *et al.*, "A novel bargaining based incentive protocol for opportunistic networks," in *Proc. IEEE GLOBECOM*, Anaheim, CA, USA, 2012, pp. 5285–5289.

[161] B. Jedari, L. Liu, T. Qiu, A. Rahim, and F. Xia, "A game-theoretic incentive scheme for social-aware routing in selfish mobile social networks," *Future Gener. Comput. Syst.*, vol. 70, pp. 178–190, May 2017.

[162] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6692–6702, Aug. 2016.

[163] L. Li, Y. Qin, and X. Zhong, "A novel routing scheme for resource-constraint opportunistic networks: A cooperative multiplayer bargaining game approach," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6547–6561, Aug. 2016.

[164] Z. Han and H. V. Poor, "Coalition games with cooperative transmission: A cure for the curse of boundary nodes in selfish packet-forwarding wireless networks," *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 203–213, Jan. 2009.

[165] K. Akkarajitsakul, E. Hossain, and D. Niyato, "Cooperative packet delivery in hybrid wireless mobile networks: A coalitional game approach," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 840–854, May 2013.

[166] R. Zhang, L. Song, Z. Han, X. Cheng, and B. Jiao, "Distributed resource allocation for device-to-device communications underlaying cellular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Budapest, Hungary, 2013, pp. 1889–1893.

[167] H. Zhu, Y. Cao, B. Liu, and T. Jiang, "Energy-aware incentive mechanism for content sharing through device-to-device communications," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–7.

[168] Y. Xiao, K.-C. Chen, C. Yuen, Z. Han, and L. A. DaSilva, "A Bayesian overlapping coalition formation game for device-to-device spectrum sharing in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 4034–4051, Jul. 2015.

[169] Y. Zhao and W. Song, "A coalitional graph game for device-to-device data dissemination with power budget constraints," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, San Francisco, CA, USA, 2017, pp. 1–6.

[170] F. Wang, Y. Li, Z. Wang, and Z. Yang, "Social-community-aware resource allocation for D2D communications underlaying cellular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3628–3640, May 2016.

[171] Y. Cai, Y. Fan, and D. Wen, "An incentive-compatible routing protocol for two-hop delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 266–277, Jan. 2016.

[172] R. El-Azouzi, F. De Pellegrini, H. B. A. Sidi, and V. Kamble, "Evolutionary forwarding games in delay tolerant networks: Equilibria, mechanism design and stochastic approximation," *Comput. Netw.*, vol. 57, no. 4, pp. 1003–1018, 2013.

[173] G. L. Cota *et al.*, "RACOON++: A semi-automatic framework for the selfishness-aware design of cooperative systems," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2017.2706286.

[174] Y. Wang, A. V. Vasilakos, and J. Ma, "VPEF: A simple and effective incentive mechanism in community-based autonomous networks," *IEEE Trans. Netw. Service Manag.*, vol. 12, no. 1, pp. 75–86, Mar. 2015.

[175] W. Chahin, H. B. A. Sidi, R. El-Azouzi, F. D. Pellegrini, and J. Walrand, "Incentive mechanisms based on minority games in heterogeneous delay tolerant networks," in *Proc. 25th Int. Teletraffic Congress (ITC)*, Shanghai, China, 2013, pp. 1–9.

[176] J. Huang *et al.*, "A game-theoretic resource allocation approach for intercell device-to-device communications in cellular networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 4, pp. 475–486, Oct./Dec. 2016.

[177] B. Barua, Z. Khan, Z. Han, A. A. Abouzeid, and M. Latva-Aho, "Incentivizing selected devices to perform cooperative content delivery: A carrier aggregation-based approach," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 5030–5045, Jul. 2016.

[178] J. Li, R. Bhattacharyya, S. Paul, S. Shakkottai, and V. Subramanian, "Incentivizing sharing in realtime D2D streaming networks: A mean field game perspective," *IEEE/ACM Trans. Netw.*, vol. 25, no. 1, pp. 3–17, Feb. 2017.

[179] T. Zhang, H. Wang, X. Chu, and J. He, "A signaling-based incentive mechanism for device-to-device content sharing in cellular networks," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1377–1380, Jun. 2017.

[180] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4628–4639, Oct. 2009.

[181] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1483–1493, Apr. 2010.

[182] H. Chen, W. Lou, Z. Wang, and Q. Wang, "A secure credit-based incentive mechanism for message forwarding in noncooperative DTNs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6377–6388, Aug. 2016.

[183] J. Zhou and Z. Cao, "TIS: A threshold incentive scheme for secure and reliable data forwarding in vehicular delay tolerant networks," in *Proc. IEEE GLOBECOM*, Anaheim, CA, USA, 2012, pp. 985–990.

[184] Y. Wang, M. C. Chuah, and Y. Chen, "Incentive based data sharing in delay tolerant mobile networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 370–381, Jan. 2014.

[185] X. Guan, C. Liu, M. Chen, H. Chen, and T. Ohtsuki, "Internal threats avoiding based forwarding protocol in social selfish delay tolerant networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, 2011, pp. 1–6.

[186] A. Mei and J. Stefa, "Give2Get: Forwarding in social mobile wireless networks of selfish individuals," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 4, pp. 569–582, Jul./Aug. 2012.

[187] Z. Ning *et al.*, "CAIS: A copy adjustable incentive scheme in community-based socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3406–3419, Apr. 2017.

[188] T. Seregina, O. Brun, R. El-Azouzi, and B. J. Prabhu, "On the design of a reward-based incentive mechanism for delay tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 2, pp. 453–465, Feb. 2017.

[189] S. Misra, S. Pal, and B. K. Saha, "Distributed information-based cooperative strategy adaptationin opportunistic mobile networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 3, pp. 724–737, Mar. 2015.

[190] X. Zhuo, W. Gao, G. Cao, and S. Hua, "An incentive framework for cellular traffic offloading," *IEEE Trans. Mobile Comput.*, vol. 13, no. 3, pp. 541–555, Mar. 2014.

[191] Y. Li *et al.*, "A contract-based incentive mechanism for delayed traffic offloading in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5314–5327, Aug. 2016.
[192] S. T. Kouyoumdjieva and G. Karlsson, "Energy-aware opportunistic mobile data offloading under full and limited cooperation," *Comput. Commun.*, vol. 84, pp. 84–95, Jun. 2016.
[193] Y. Zhang, L. Song, W. Saad, Z. Dawy, and Z. Han, "Contract-based incentive mechanisms for device-to-device communications in cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2144–2155, Oct. 2015.
[194] Y. Chen, S. He, F. Hou, Z. Shi, and J. Chen, "Promoting device-to-device communication in cellular networks by contract-based incentive mechanisms," *IEEE Netw.*, vol. 31, no. 3, pp. 14–20, May/Jun. 2017.
[195] Y. Pan *et al.*, "On consideration of content preference and sharing willingness in D2D assisted offloading," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 4, pp. 978–993, Apr. 2017.
[196] B. Jedari *et al.*, "A social based watchdog system to detect selfish nodes in opportunistic mobile networks," *Future Gener. Comput. Syst.*, Nov. 2017, doi: 10.1016/j.future.2017.10.049.

Behrouz Jedari, photograph and biography not available at the time of publication.

Feng Xia, photograph and biography not available at the time of publication.

Zhaolong Ning, photograph and biography not available at the time of publication.